CSC 281

* **Proposition**: A proposition it's statement that is either True or False. (but not both)

"1+1=2" ← proposition
"1+3=10" ← proposition
"Jeddah is the capital of Saudi Arabia" ← proposition

"How are you?" ← not proposition
"Who are you?" ← not proposition
"1+x=5" not proposition until we know the value of x.

Complex Statement:

$P_1\ P_2\ P_3\ \cdots\ P_n$

operations: AND ($\wedge$), OR ($\vee$), XOR ($\oplus$), XNOR ($\overline{\oplus}$), implication ($\rightarrow$)

Negation: $\neg$

Truth Table:

$P_1 \wedge P_2$

P_1	P_2	$P_1 \wedge P_2$	$P_1 \rightarrow P_2$
T	T	T	T
T	F	F	F
F	T	F	T
F	F	F	T

Tautology: a statement that is always true.

Ex. $p \vee (\neg p) \iff T$

contradiction: a statement that is always false.

Ex. $p \wedge (\neg p) \iff F$

* **converse**: $p \rightarrow q$ is $q \rightarrow p$
Contrapositive: $p \rightarrow q$ is $\neg q \rightarrow \neg p$
Biconditional: $p \leftrightarrow q$ is $p \rightarrow q \wedge q \rightarrow p$

Ex. Show that $p \to q$ and $\neg p \vee q$ are logically equivalent.

p	q	$p \to q$	$\neg p \vee q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

* Logical Equivalent:

(1) identity laws: $p \wedge T \Leftrightarrow p$ $\quad p \vee F \Leftrightarrow p$

(2) domination laws: $p \vee T \Leftrightarrow T$ $\quad p \wedge F \Leftrightarrow F$

(3) idempotent laws: $p \wedge p \equiv p$ $\quad p \vee p \equiv p$

(4) double negation law: $\neg(\neg p) \equiv p$

(5) commutative laws: (1) $p \wedge q \equiv q \wedge p$ (2) $p \vee q \equiv q \vee p$

(6) Associative laws: (1) $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

(2) $(p \vee q) \vee r \equiv p \vee (q \vee r)$

(7) Distributive laws: (1) $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

(2) $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

(8) Demorgan's laws: (1) $\neg(p \wedge q) \equiv \neg p \vee \neg q$

(2) $\neg(p \vee q) \equiv \neg p \wedge \neg q$

(9) Conditional law: $p \to q \equiv \neg p \vee q$

Ex. Show that $\neg(p \vee (\neg p \wedge q))$ and $\neg p \wedge \neg q$ are logically Equivalent.

Sol.
$$\begin{aligned}\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) \\ &\equiv \neg p \wedge (p \vee \neg q) \\ &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) \\ &\equiv F \vee (\neg p \wedge \neg q) \\ &\equiv \neg p \wedge \neg q\end{aligned}$$

Ex. Determine if $\neg(p \wedge (p \to q)) \to \neg q$ is tautology.

Sol.
$$\begin{aligned}\neg(p \wedge (p \to q)) \to \neg q &\equiv (p \wedge (p \to q)) \vee \neg q \\ &\equiv (p \wedge (\neg p \vee q)) \vee \neg q \\ &\equiv ((p \wedge \neg p) \vee (p \wedge q)) \vee \neg q \\ &\equiv (F \vee (p \wedge q)) \vee \neg q \\ &\equiv (p \wedge q) \vee \neg q \\ &\equiv (\neg q \vee p) \wedge (\neg q \vee q) \\ &\equiv (\neg q \vee p) \wedge T \\ &\equiv \neg q \vee p\end{aligned}$$

is not tautology

* Proposition Function:

Let $P(x) =$ "$x + 5 = 10$"

$P(1)$ is false

$P(5)$ is true

$P(-3)$ is False

Let $Q(x, y) = x > y$

$Q(1, 1)$ is false

$Q(10, 2)$ is true

* Assigning values to variable *

- Direct
- universal quantifier ($\forall$)
- Essential quantifier ($\exists$)

→ universe of discourse : شي

Ex. let $P(x) = x+5=10$, and let universe of discourse is $\mathbb{R}$.

Sol.

$\forall x\ P(x)$ is False.

$\exists x\ P(x)$ is True.

* suppose universe of discourse is $\{x_1, x_2, \dots, x_n\}$, so:

$$\forall x\ P(x) \Rightarrow P(x_1) \wedge P(x_2) \wedge \dots \wedge P(x_n)$$

$$\exists x\ P(x) \Rightarrow P(x_1) \vee P(x_2) \vee \dots \vee P(x_n)$$

Ex. let $P(x) = x \geq 0$, universe of discourse is $\mathbb{R}$.

Sol.

$\forall x\ P(x)$ is False

let universe of discourse is $\mathbb{Z}^+$ (positive integers),

$\forall x\ P(x)$ is True

Ex. let $Q(x,y) = x+y > 10$, let universe of discourse is $\mathbb{Z}$ (positive and negative integers)

Sol.

False $\forall x \forall y\ Q(x,y) \equiv \forall y \forall x\ Q(x,y)$

True $\exists x \exists y\ Q(x,y) \equiv \exists y \exists x\ Q(x,y)$

True $\forall x \exists y\ Q(x,y) \not\equiv \exists y \forall x\ Q(x,y)$

False $\exists x \forall y\ Q(x,y) \not\equiv \forall y \exists x\ Q(x,y)$

- Expressing English sentence using predicate functions and quantifiers:

Ex: Let $F(x,y)$ = "y is father of x"

Ali is father of bilal.

$F(Bilal, Ali) \Rightarrow$ True

$F(Ali, Bilal) \Rightarrow$ False

"Every person has a father"

universe of discourse = All humans

"Every person has a single father"

$\forall x \exists y \forall z \; (F(x,y) \wedge z \neq y \rightarrow \neg F(x,z))$

* Negating quantifiers:

$$\neg(\forall x\ P(x)) \iff \exists x\ \neg P(x)$$

Ex. Let $P(x)$ = "x speaks Arabic"

universe of discourse = all Students in this class

$\neg(\forall x\ P(x))$

$$\neg(\exists x\ P(x)) \iff \forall x\ \neg P(x)$$

---

* Sets: a collection of objects.

$A = \{1,2,3\}$ $\quad |A| = 3$

$B = \{\text{Honda}, \text{BMW}\}$ $\quad |B| = 2$

$C = \{1, a, \square\}$ $\quad |C| = 3$

* cardinality of a set: size (# elements) in the set.

$D = \{1, a, \{7,8,6\}, b\}$ $\quad |D| = 4$

$1 \in D$ $\quad 7 \notin D$ $\quad \{7,8,6\} \in D$

* Empty set: $\emptyset$: $\{\}$

subsets

subset: $E \subseteq D$ $\quad |E| \leq |D|$

proper set: $F \subset D$ $\quad |F| < |D|$

$D = \{1, a, \{7,8,6\}, b\}$

D تحتوي على جميع عناصر E ← تكون E

$\forall x\ (x \in E \rightarrow x \in D)$ تعريف الـ subset

مثال على العكس ←

$E = \{1, a\}$

$F = \{b\}$

* powerset : set of all subsets.

$A = \{1, 2, 3\}$

$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

* $|P(A)| = 2^{|A|}$
* $P(\emptyset) = \{\emptyset\}$
* $P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$

$D = \{1, a, \{7,8,6\}, b\}$

element $a \in D$

$\{a\} \notin D$

subset $\{a\} \subseteq D$

$P(D) = \{\emptyset, \{1\}, \{a\}, \{\{7,8,6\}\}, \{b\}, \{1,a\}, \{1, \{7,8,6\}\}, \{1,b\}, \{a, \{7,8,6\}\}, \{a,b\}, \{\{7,8,6\}, b\}, \{1, a, \{7,8,6\}\}, \{1,a,b\}, \{a, \{7,8,6\}, b\}, \{1, a, \{7,8,6\}, b\}, \{1, \{7,8,6\}, b\}\}$

* Cartesian Product of sets:

$A \times B = \{(x,y) \mid x \in A \wedge y \in B\}$

* $A \times B \neq B \times A$
* $|A \times B| = |A| \cdot |B|$

$A = \{1,2,3\}$, $B = \{a,b\}$

$A \times B = \{(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)\}$

$(1,b) \in A \times B$

* $A \times \emptyset = \emptyset$

set Operations

- Difference
- Complement
- Union
- Intersection

$A \cup B = \{x \mid x \in A \vee x \in B\}$

$A \cap B = \{x \mid x \in A \wedge x \in B\}$

$\bar{A} = \{x \mid x \notin A\}$

$A - B = \{x \mid x \in A \wedge x \notin B\}$

Ex: $A = \{1, a, 3\}$, $B = \{2, b, 3\}$

sol. $A \cup B = \{1, 2, 3, a, b\}$

$A \cap B = \{3\}$

$A - B = \{1, a\}$

* Set Identifiers:

* U = universal set.

(1) identity laws:

$A \cup \emptyset = A$

$A \cap U = A$

(2) Domination laws:

$A \cup U = U$

$A \cap \emptyset = \emptyset$

(3) Idempotent laws:

$A \cup A = A$

$A \cap A = A$

(4) Double complement law:

$\bar{\bar{A}} = A$

(5) Commutative laws:

$A \cup B = B \cup A$

$A \cap B = B \cap A$

(6) Associative laws:

$(A \cup B) \cup C = A \cup (B \cup C)$

$(A \cap B) \cap C = A \cap (B \cap C)$

(7) Distributive laws:

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(8) DeMorgan laws:

$\overline{A \cup B} = \bar{A} \cap \bar{B}$

$\overline{A \cap B} = \bar{A} \cup \bar{B}$

How to prove set $A = B$?

(1) Show $A \subseteq B$

(2) Show $B \subseteq A$

* Prove $\overline{A \cap B} = \bar{A} \cup \bar{B}$

① First, we show $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:

let $x \in \overline{A \cap B} \Rightarrow x \notin A \cap B \Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \in \bar{A}$ or $x \in \bar{B}$

$\Rightarrow x \in \bar{A} \cup \bar{B}$

② Next, we show $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$:

let $x \in \bar{A} \cup \bar{B} \Rightarrow x \in \bar{A}$ or $x \in \bar{B}$

$\Rightarrow x \notin A$ or $x \notin B$

$\Rightarrow x \notin A \cap B$

$\Rightarrow x \in \overline{A \cap B}$

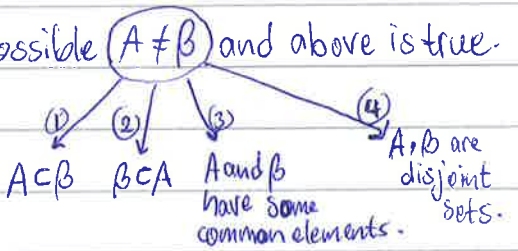
Ex. Given sets A, B, C. if $A \cup C = B \cup C$

$A \cap C = B \cap C$

Does it mean that $A = B$?

Sol.

we show it's not possible $(A \neq B)$ and above is true.



① let $A \subset B$:

Assume $x \in B$ and $x \notin A$

$A \cup C = B \cup C \Rightarrow x \in C$

$A \cap C = B \cap C \Rightarrow x \notin C$

$\Rightarrow A \notin B$

② same as ①

③ let A, B set with some common elements:

$x \in A \cap B$

$\alpha \in A$, $k \in B$, and $\alpha \notin A \cap B$

$k \notin A \cap B$

$A \cup C = B \cup C \Rightarrow \alpha \in C$ and $k \in C$

$A \cap C = B \cap C \Rightarrow \alpha \notin C$ and $k \notin C$

} Not possible

Ex. Given sets A, B, C

if $A \cup C = B \cup C$

$A \cap C = B \cap C$

Does this implies that $A = B$

proof by contradiction.

Sol. Assume $A \neq B$

④ A, B are disjoint sets.

$A \cup C = B \cup C \Rightarrow A \subset C$ and $B \subset C$

$A \cap C = B \cap C \Rightarrow A \not\subset C$ and $B \not\subset C$

$A \neq B$ not possible,

so $A = B$

* Another Proof:

$$A \cup (A \cap C) = A \cup (B \cap C)$$

$$= A$$

$$= (A \cup B) \cap (A \cup C)$$

$$= (A \cup B) \cap (B \cup C)$$

$$= ((A \cup B) \cap B) \cup ((A \cup B) \cap C)$$

$$= B \cup ((C \cap A) \cup (C \cap B))$$

$$= B \cup (C \cap B)$$

$$= B$$

so $A = B$

* Extensions:

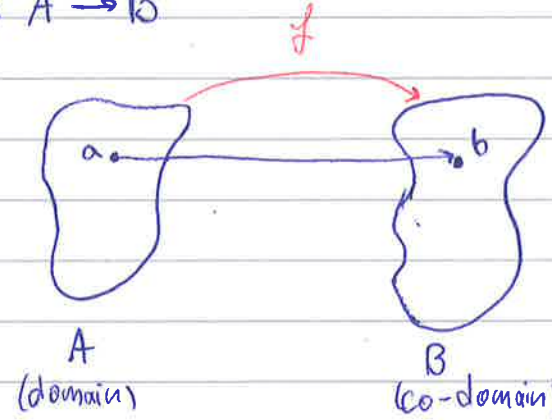
① Multi Sets: Allows duplicate elements. $A = \{a \cdot 2, b \cdot 3\}$

② Fuzzy Sets: Each element has degree of belonging.

Functions

Function f is a mapping between elements of two sets.

$f: A \to B$



$f(a) = b$

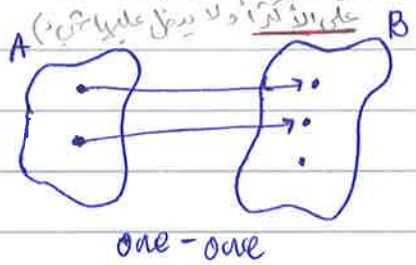
pre-image of b under f.

image of a under f

Types of Functions ($f: A \to B$)

one-one

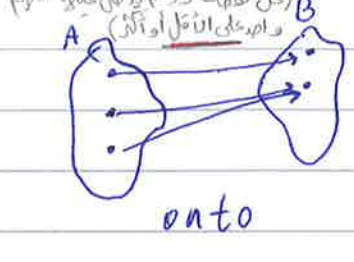
$\forall a, b \in A \ni f(a) = f(b) \Leftrightarrow a = b$



one-one

onto

$\forall b \in B$ is an image of some $a \in A$



onto

1-1 correspondence

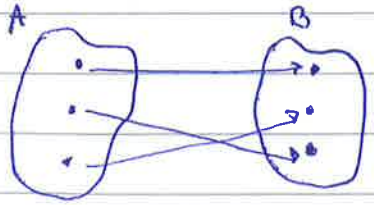
one-one and onto

every element has an inverse

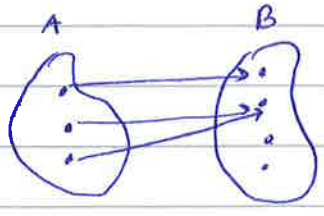
inverse: $f^{-1}: B \to A$

Neither

(not any of the previous ones)



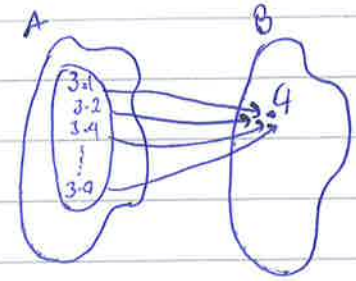
1-1 correspondence



Neither

Ex. $g: \mathbb{R} \to \mathbb{Z}$ $\quad g(x) = \lceil x \rceil$ (ceiling)

Sol. is onto, because



1-1 correspondence (تقابل)

Ex. $f(x) = 3x+2$

Sol. 1-1 correspondence

composition:

$f(x)$ $g(x)$

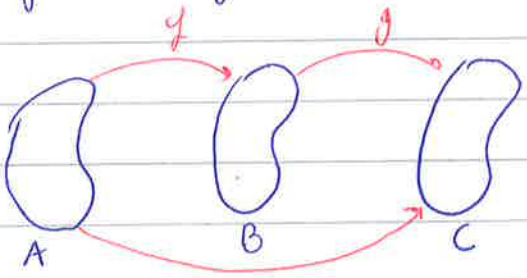
$(f \circ g)(x) = f(g(x))$

$(g \circ f)(x) = g(f(x))$

$f: A \to B$, $g: B \to C$

$(f \circ g)(x) = f(g(x))$ not defined

$(g \circ f)(x) = g(f(x))$ defined



Ex. $f: \mathbb{R} \to \mathbb{R}$ $\quad f(x) = 3x^2+5$

$g: \mathbb{R} \to \mathbb{R}$ $\quad g(x) = \sqrt{x-1}$

Sol.

$(f \circ f)(x) = f(3x^2+5) = 3(3x^2+5)^2+5$

$(g \circ f)(x) = g(3x^2+5) = \sqrt{(3x^2+5)-1}$

$(f \circ g)(x) = f(\sqrt{x-1}) = 3(\sqrt{x-1})^2+5 = 3(x-1)+5$

$(g \circ g)(x) = g(\sqrt{x-1}) = \sqrt{(\sqrt{x-1})-1}$

* $f: \mathbb{R} \to \mathbb{Z}$
  $g: \mathbb{Z} \to \mathbb{Z}$
  it just defined for $(g \circ g)(x)$ & $(g \circ f)(x)$

Sequences:

* Mapping between $\mathbb{Z}^+$ or $\mathbb{N}$ (0 or 1) to $\mathbb{R}$

sequence: $a_1, a_2, a_3, a_4, \cdots$

// : $b_0, b_1, b_2, b_3, \cdots$

Ex. $\{a_n\}_{n \geq 1} = 2n+3$

Sol.

sequence (terms) = $5, 7, 9, 11, 13, \cdots$

$\{b_n\}_{n \geq 0} = 3x^2-1$

Sol. $= -1, 2, 11, \cdots$

types of sequence: ① arithmetic sequence: constant difference between terms.

② geometric sequence: constant ratio between terms.

Arithmetic sequence:

$$a_n = a_1 + (n-1) \times d$$

a_1: first term; d: constant difference

Ex. given sequence: 7, 13, 19, 25, ---- (d = 6, 6, 6)

① What is a_{100}.

② " " a_n.

③ " term the sequence exceeds 1000.

Sol.

① $a_{100} = 7 + 99 \times 6 = \underline{601}$

② $a_n = 7 + (n-1) \times 6 = \underline{6n+1}$

③ Find smallest n such that $6n+1 > 1000$

$$n > \frac{1000-1}{6} \longrightarrow n = \frac{\lceil 999 \rceil}{6} = \underline{167}$$

لأن n صحيحة أنظر عدد صحيح

so it's: a_{167}

Ex. given $a_{57} = 212$, $a_{58} = 216$, $a_{59} = 220$ (d = 4, 4), Find a_{10}

Sol.

$a_{57} = a_1 + 56 \times 4$ (a_1: ?)

$\therefore a_1 = 212 - 56 \times 4 = -12$

$\therefore a_{10} = -12 + 9 \times 4$

$= \underline{24}$

Geometric sequence:

ratio ⟶ number

Ex. Find the next term in the sequence: 1, 7, 25, 79, ?

Sol.

ratio

$\frac{25}{7} = 3.57$

$\frac{79}{25} = 3.16$

ratio → 3 (approximately)

$a_5 = 3^5 - 2$
$= 241$

Formula:

$a_n = 3^n \pm ? - 2 \quad n \geq 1$

n	0	1	2	3	4	...
3^n	1	3	9	27	81	

Ex. Consider the sequence: 4, 5, 7, 11, 19, 35, 67, ?

a_0

Sol.

ratio → 2

$\frac{7}{5} = 1.4$ $\quad \frac{11}{7} = 1.57$

$\frac{19}{11} = 1.72$ $\quad \frac{35}{19} = 1.84$

$a_7 = 2^7 + 3$
$= 131$

Formula:

$a_n = 2^n \pm ?$
$= 2^n + 3 \quad n \geq 0$

n	0	1	2	3	4	5	...
2^n	1	2	4	8	16	32	

* Summation:

① $\sum_{i=1}^{n} a_i = a_1 + a_2 + a_3 + \cdots + a_n$

② $\sum_{i=1}^{n} c = c + c + c + \cdots + c = \boxed{cn}$

③ $\sum_{i=m}^{n} c = c + c + c + \cdots + c$
$= \boxed{c \times (n - m + 1)}$

④ $\sum_{i=1}^{n} i = \boxed{1 + 2 + 3 + \cdots + n}$ (= S)
$= \boxed{\frac{n(n+1)}{2}}$

كيفية استنتاج القانون:

let:

$S = 1 + 2 + 3 + \cdots + n$ (تصاعدي)

$+ \quad S = n + (n-1) + (n-2) + \cdots + 1$ (تنازلي)

(كل حد = n+1)

$2S = n \times (n+1)$

$S = \frac{n(n+1)}{2}$

- Calculate:

⑤ $\sum_{i=m}^{n} i =$ Sol.

$m+(m+1)+\cdots+n$

Add $1+2+3+\cdots+(m-1)$

$= \sum_{i=1}^{n} i$

$\frac{1}{2}n(n+1)$

Substract $1+2+3+\cdots+(m-1)$

$= -\sum_{i=1}^{m-1} i$

$-\frac{1}{2}(m-1)\times m$

$= \frac{1}{2}[n^2+n-m^2+m]$

⑥ $\sum_{i=1}^{n} i^2 = 1^2+2^2+3^2+\cdots+n^2$

$= \frac{n(n+1)(2n+1)}{6}$

- Calculate:

$\sum_{i=m}^{n} i^2 = \sum_{i=1}^{n} i^2 - \sum_{i=1}^{m-1} i^2$

$= \frac{n(n+1)(2n+1)}{6} - \frac{m(m-1)(2m-1)}{6}$

Ex. Calculate $\sum_{\substack{i=50 \\ i=\text{odd}}}^{100} i = 51+53+55+\cdots+99$

Sol.

Formula to generate odd integers.

$2k+1 \qquad k \in \mathbb{Z}$

$\sum_{\substack{i=50 \\ i=\text{odd}}}^{100} i = \sum_{k=25}^{49} (2k+1)$

Let $2k+1 = 51$

$k = 25$

$2k+1 = 99$

$k = 49$

$\sum_{k=25}^{49} (2k+1) = 2\sum_{k=25}^{49} k + \sum_{k=25}^{49} 1$

$= 2\times\frac{1}{2}[49\times 50 - 24\times 25] + (49-25+1)\times 1$

$= 1875$

$\sum_{\substack{i=50 \\ i=\text{odd}}}^{100} i =$

Ex. $\sum_{i=1}^{n}\underbrace{\sum_{j=1}^{m} i}_{=m\times i}$ (حاصل ثابت بالأمل)

$= m\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)\times m$

Ex. $\sum_{i=1}^{n}\underbrace{\sum_{j=1}^{m} j}_{=\frac{1}{2}m(m+1)}$

$= \frac{1}{2}m(m+1)\cdot\sum_{i=1}^{n}1$

$= \frac{1}{2}m(m+1)\times n$

Ex. $\sum_{i=1}^{n}\underbrace{\sum_{j=1}^{i} j}_{=\frac{1}{2}i(i+1)}$

$= \frac{1}{2}\sum_{i=1}^{n} i^2+i$

$= \frac{1}{2}\left[\sum_{i=1}^{n} i^2 + \sum_{i=1}^{n} i\right]$

$= \frac{1}{2}\left[\frac{n(n+1)(2n+1)}{6} + \frac{1}{2}n(n+1)\right]$

$= \frac{1}{2}n(n+1)\left[\frac{2n+1}{3}+1\right]$

Ex. $\sum_{i=1}^{n}\underbrace{\sum_{j=i}^{m} j}_{=\frac{1}{2}[m(m+1)-i(i-1)]}$

$= \frac{1}{2}\left[\sum_{i=1}^{n} m(m+1) - \sum_{i=1}^{n} i^2 + \sum_{i=1}^{n} i\right]$

$= \frac{1}{2}\left[n\times m(m+1) - \frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2}\right]$

Ex. Calculate $\sum_{i=0}^{n} r^i = 1+r+r^2+r^3+\cdots+r^n$ (geometric sequence)

Sol.

$$= \frac{r^{n+1}-1}{r-1}$$

Proof Let $S = 1+r+r^2+r^3+\cdots+r^n$ — ①

$rS = r+r^2+r^3+\cdots+r^{n+1}$ — ②

② − ①

$rS - S = r^{n+1} - 1$

$S(r-1) = r^{n+1}-1$

$\therefore S = \frac{r^{n+1}-1}{r-1}$

$$\sum_{i=m}^{n} r^i = \frac{r^{n+1}-r^m}{r-1}$$

(كرناني هود ضرب سوية)

(big pi) product sign ↘

$$\prod_{i=1}^{n} c = c \times c \times c \times \cdots \times c = \boxed{c^n}$$

$$\prod_{i=m}^{n} c = \boxed{c^{n-m+1}}$$

$$\prod_{i=m}^{n} ci = \prod_{i=m}^{n} c \times \prod_{i=m}^{n} i$$

$$\prod_{i=1}^{n} i = 1 \times 2 \times 3 \times \cdots \times n = \boxed{n!}$$

Def. a, b integers → $b = ax$ for some integer x.

$a \mid b$ "a divides b" Ex. $2 \mid 10$ $3 \mid 18$ $7 \mid 28$

$a \nmid b$ "a does not divide b" Ex. $2 \nmid 9$ $3 \nmid 17$ $7 \nmid 20$

→ $b \neq ax$ for all integers x

Th a, b, c integers, Then:

① if $a \mid b$ (let $b = ax$) and $a \mid c$ (let $c = ay$, y some integer) then $a \mid (b+c)$.

$b + c = ax + ay \Rightarrow b + c = a(x+y)$ (integer)

$\therefore a \mid (b+c)$

② if $a \mid b$ then $a \mid bc$.

③ if $a \mid b$ and $b \mid c$ then $a \mid c$.

let $b = ax$ for x some integers

$bc = axc$ (integer) $\therefore a \mid bc$

$a \mid b \Rightarrow$ let $b = ax$ x some integer

$b \mid c \Rightarrow$ let $c = by$ y " "

$c = axy$ (integer) $\Rightarrow \therefore a \mid c$

Def. An integer P is called prime if it's only divisors are 1 and itself.

Ex. 2, 3, 5, 7, 11, 13, ...

Def. An integer is composite if it is not prime.

Ex. 4, 6, 8, 9, 10, 12, ...

Th. Any integer can be written uniquely as product of primes.

$15 = 3 \times 5$

$16 = 2 \times 2 \times 2 \times 2$

$17 = 17$ → (تحليل يعتبر إجابة لأن 17 أولي)

$18 = 2 \times 3^2$

Ex. How to determine if a number n is prime?

Sol.

Th. Any composite integer n has a prime divisor $\leq \sqrt{n}$

$\lfloor \sqrt{59} \rfloor \sim 7$

$2 \nmid 59$

$3 \nmid 59$

$5 \nmid 59$

$7 \nmid 59$

Th. A number P is prime if it does not have a divisor $\leq \sqrt{p}$

Proof: n composite.

such that (بحيث أن)

$\exists$ integers $a, b \ni n = ab$

$\ni 1 < a < n$

$1 < b < n$

claim:

$a \leq \sqrt{n}$ or $b \leq \sqrt{n}$

(نجرب صحة نفيها) otherwise (o/w):

$a > \sqrt{n}$ ~~or~~ and $b > \sqrt{n}$

$\Rightarrow n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$ (وهذا خاطئ)

∴ الادعاء صحيح

Ex. ① Given number n. Is n prime? } n is Prime if $\nexists$ a prime factor $\leq \sqrt{n}$

↓

Ex. $n = 269$

Sol. $\sqrt{269} \sim 18$ ← floor سويناله

$2 \nmid 269$

$3 \nmid 269$

$5 \nmid 269$

$7 \nmid 269$

$11 \nmid 269$

$13 \nmid 269$

$17 \nmid 269$

} 269 is prime.

stop since

$19 > \sqrt{269}$

(2) if not, what is its prime divisors.

Ex Find prime factor of $n = 7692 = 2^2 \times 3 \times 641$

Sol.

$\sqrt{7692} \sim 87$

$2 \mid 7692$ $\quad \frac{7692}{2} = 3846$

$2 \mid 3846$ $\quad \frac{3846}{2} = 1923$

$2 \nmid 1923$

$3 \mid 1923$ $\quad \frac{1923}{3} = 641$

$3 \nmid 641$

$5 \nmid 641$

$7 \nmid 641$

$11 \nmid 641$

$13 \nmid 641$

$17 \nmid 641$

$19 \nmid 641$

$23 \nmid 641$ → stop 29 > $\sqrt{641}$

~~$29 \nmid 641$~~

Greatest Common Divisor

Def. Integers a, b.

The greatest common Divisor is the largest integer d ∋ d|a and d|b.

we say $d = \gcd(a,b)$.

Ex Find gcd(24, 36).

Sol.

Divisors of 24 : 1, 2, 3, 4, 6, 8, 12

" " 36 : 1, 2, 3, 4, 6, 9, 12, 18

gcd

Def. if $\gcd(a,b)=1$, then a and b are relatively prime.

Ex $\gcd(3,7)=1$
$\gcd(4,25)=1$

Def. Integers
$a_1, a_2, a_3, \cdots, a_n$
if $\gcd(a_i,a_j)=1$
$\forall\ i \neq j$
we say these numbers are pairwise relatively prime.

Ex 2, 11, 15
$\gcd(2,11)=1$
$\gcd(2,15)=1$
$\gcd(11,15)=1$
} pairwise relatively prime

Ex 3, 10, 25
$\gcd(3,10)=1$
$\gcd(3,25)=1$
$\gcd(10,25)=5$
} not pairwise relatively prime

* calculating $\gcd(a,b)$:

Let $a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n} = \prod_{i=1}^{n} p_i^{\alpha_i}$

$b = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_n^{\beta_n} = \prod_{i=1}^{n} p_i^{\beta_i}$

$p_1, p_2, \cdots$ Primes

$\alpha_1, \alpha_2, \cdots \geq 0$

$p_1, p_2, \cdots$ primes

$\beta_1, \beta_2, \cdots \geq 0$

$\therefore \gcd(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)}$ (min: minimum) $\Longrightarrow$ This eq. satisfies:

① divides a and b.

② greatest number that divides both.

Ex
$24 = 2^3 \times 3$
$36 = 2^2 \times 3^2$
$\gcd(24,36) = 2^2 \times 3^1 = 12$

Least common multiple (lcm)

Def. Integers a, b. then, the least common multiple is the smallest integer ℓ $\ni$ $a|\ell$ and $b|\ell$.

$$\ell = lcm(a,b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$$

Proof:

(1) show that $a|\ell$ and $b|\ell$

(2) show that there does not exist $\ell' < \ell$ such that $a|\ell'$ and $b|\ell'$

Ex:

$lcm(2,3) = 6$

$lcm(4,3) = 12$

Ex: $a = 2^3 \times 3 = 24 = 2^3 \times 3^1 \times 7^0$

$b = 2 \times 7 = 14 = 2^1 \times 3^0 \times 7^1$

$gcd(24,14) = 2^1 \times 3^0 \times 7^0 = 2$ (أخذ الأس الأصغر)

$lcm(24,14) = 2^3 \times 3^1 \times 7^1 = 168$ (أخذ الأس الأكبر)

$24 \times 14 = 2 \times 168$ (gcd, lcm)

Th: Integers a, b. then, $a \times b = gcd(a,b) \times lcm(a,b)$.

Proof:

$$gcd(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$$

$$lcm(a,b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$$

$$gcd(a,b) \times lcm(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i)} \times \prod_{i=1}^{n} p_i^{\max(\alpha_i,\beta_i)}$$

$$= \prod_{i=1}^{n} p_i^{\min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i)} \quad \min(\alpha_i,\beta_i) + \max(\alpha_i,\beta_i) = \alpha_i + \beta_i$$

$$= \prod_{i=1}^{n} p_i^{\alpha_i+\beta_i} = \prod_{i=1}^{n} p_i^{\alpha_i} \times p_i^{\beta_i} = \prod_{i=1}^{n} p_i^{\alpha_i} \times \prod_{i=1}^{n} p_i^{\beta_i} = a \times b$$

Modular Arithmetic

mod

≡

≠

Def: Integer a,

Integer ← $m > 0$

we denote the unique remainder of $\frac{a}{m}$ by $a \bmod m$.

unique ← $0 \leq \ldots < m$

Ex: $12 \bmod 4 = 0$

$12 \bmod 5 = 2$

$-12 \bmod 5 =$ → $-12 = \boxed{-3} \times 5 + \boxed{3}$ → $= 3$

نحل المعادلة

طريقة أخرى لأن

هنا باقي القسمة سيضع

سالب معرفتا البوتيك

على أنه بين $0 \leq \ldots < m$

? $0 \ldots 4$

$\frac{a}{m}$

quotient (q)

remainder (r)

$28 \bmod 5 = \overset{q}{\square} \times 5 + \overset{r}{\square}$

$0 \leq r < m$

Def: a, b Integers

m Integer > 0

then $a \equiv b \bmod m \iff m \mid (a-b)$

congruent (يتوافق)

Ex: $2 \equiv 2 \bmod 5$

$2 \not\equiv 4 \bmod 3$

$a \not\equiv b \iff m \nmid (a-b)$

Th: If $a \equiv b \bmod m$ then, $a = b + km$ for some integer k.

Proof:

$m \mid (a-b) \iff a - b = mk$ for some integer k.

Modular Arithmetic:

(الحسابية في الأعداد الصحيحة)

Let $a = bq + r \quad 0 \le r < b$

r: unique remainder

(1) $a \bmod m = r$

the unique remainder of dividing $\frac{a}{m}$

(2) $a \equiv b \bmod m \iff m \mid (a-b) \iff a \bmod m = b \bmod m$ (if and only if)

$a \not\equiv b \bmod m \iff m \nmid (a-b) \iff a \bmod m \neq b \bmod m$

(3) if $a \equiv b \bmod m \iff a = b + km$ for some integer k

proof:

(1) Given $a \equiv b \bmod m$ then $a \bmod m = b \bmod m$

($a \equiv b \bmod m$: $a = b + km$ for some integer k)

$$a \bmod m = (b + km) \bmod m \quad (km \bmod m = 0)$$
$$= (b \bmod m + km \bmod m) \bmod m$$
$$= b \bmod m$$

(إثبات طرفة وعرة فقط، والباقية نفس طريقة الإثبات)

Th. (4) Integers a, b, c, d, $m > 0$

if $a \equiv b \bmod m$ (① $a = b + k_1 m$ for some integer k_1)

$c \equiv d \bmod m$ (② $c = d + k_2 m$ // // // k_2)

then $(a+c) \equiv (b+d) \bmod m$

$a \times c \equiv b \times d \bmod m$

Proof:

$a + c = b + d + m(k_1 + k_2)$ (① + ②)

$(a+c) - (b+d) = m(k_1 + k_2)$

$\therefore m \mid ((a+c) - (b+d))$ (integer)

or $(a+c) \equiv (b+d) \bmod m$

$a \times c = b \times d + m(k_1 d + k_2 b + k_1 k_2 m)$ (① × ②)

$ac - bd = m(k_1 d + k_2 b + k_1 k_2 m)$

(integer)

$\therefore m \mid (ac - bd)$

or $ac \equiv bd \bmod m$

*Lemma:

let $a = bq + r$ (unique reminder) $\quad 0 \le r < b$ $\quad b, q, a$ are integers

then

$\gcd(a,b) = \gcd(b,r)$ {Euclidean Algorithm for computing gcd}

Proof:

consider integers a, b

Let $d \mid a$ and $d \mid b$ — d is absolutly an integer.

$d \mid ax$ For all integer $x \in \mathbb{Z}$

$d \mid by$ For all integer $y \in \mathbb{Z}$

$\therefore d \mid (ax + by) \quad x, y \in \mathbb{Z}$

Let $x = 1$, $y = -q$ $\Rightarrow d \mid (a - bq) \Rightarrow \therefore d \mid r$ ($a - bq = r$)

$\therefore$ common divisor of a and b is also common divisor of b and r.

*How to calculate $\gcd(a,b)$:

*Euclidean Algorithm for gcd: Appiy above Lemma till reminder=0.

$a = bq + r \quad 0 \le r < b \quad \gcd(a,b) = \gcd(b,r)$

$b = rq' + r' \quad 0 \le r' < r \quad \gcd(b,r) = \gcd(r,r')$

$r = r'q'' + r'' \quad 0 \le r'' < r' \quad \gcd(r,r') = \gcd(r;r'')$

كل مرة نقسم لحسان إلى أن نصل لباقي صفر ثم نتوقف ونكتب الحل.

$+ \overline{0}$

* وال gcd هو آخر باقي قسمة قبل الصفر.

Ex: $\gcd(662, 24)$ =

sol.

$662 = \boxed{27} \times 24 + \boxed{14}$

$24 = \boxed{1} \times 14 + \boxed{10}$

$14 = \boxed{1} \times 10 + \boxed{4}$

$10 = \boxed{2} \times 4 + \boxed{2}$

$4 = \boxed{2} \times 2 + \boxed{0}$

gcd

Ex: gcd(664, 414).

sol:

$664 = 1 \times 414 + 250$
$414 = 1 \times 250 + 164$
$250 = 1 \times 164 + 86$
$164 = 1 \times 86 + 78$
$86 = 1 \times 78 + 8$
$78 = 9 \times 8 + 6$
$8 = 1 \times 6 + 2$
$6 = 3 \times 2 + 0$

gcd

$2 = 8 - 1 \times 6$
$= 8 - 1 \times (78 - 9 \times 8)$
$= -1 \times 78 + 10 \times 8$
$= -1 \times 78 + 10 \times (86 - 1 \times 78)$
$= 10 \times 86 - 11 \times 78$
$= 10 \times 86 - 11 \times (164 - 1 \times 86)$
$= -11 \times 164 + 21 \times 86$
$= -11 \times 164 + 21 \times (250 - 1 \times 164)$
$= 21 \times 250 - 32 \times 164$
$= 21 \times 250 - 32 \times (414 - 1 \times 250)$
$= -32 \times 414 + 53 \times 250$
$= -32 \times 414 + 53 \times (664 - 1 \times 414)$
$= 53 \times 664 - 85 \times 414$

Conversion of number into different bases

Ex: $2305_7 = 1011001_2$ (convert to base 10, then convert to base 2)

sol:

$(5 \times 7^0) + (0 \times 7^1) + (3 \times 7^2) + (2 \times 7^3) = 838_{10}$

838 ÷3 → 279 (1), 279 ÷3 → 93 (0), 93 ÷3 → 31 (0), 31 ÷3 → 10 (1), 10 ÷3 → 3 (1), 3 ÷3 → 1 (0), 1 (1)

Ex: $56_{10} = ?_3$ ∴ $= 2002_3$

sol:

56 ÷3 → 18 (2), 18 ÷3 → 6 (0), 6 ÷3 → 2 (0), 2 (2)

reminder

Ex: $251_{10} = 506_7$

sol:

convert to base 7

251 ÷7 → 35 (5), 35 ÷7 → 5 (0), 5 (6)

$251 \div 7 = 35.857 \Rightarrow 0.857 = 5.999 = 6$

base 7

Ex: $134_5 = ?_7 = 62_7$

sol:

we find first $134_5 = ?_{10}$, then we find $?_{10} = ?_7$.

$134_5 = 44_{10}$

$(4 \times 5^0) + (3 \times 5^1) + (1 \times 5^2)$

44_{10} ÷7 → 6 (6), 2 (2)

we stop here because 6 is less than the base 7.

$44_{10} = 62_7$

Expressing gcd as a linear combination of its arguments.

$$\gcd(a,b) = \text{---} \times a + \text{---} \times b$$

$$\gcd(664, 414) = 2 = \text{---} \times 664 + \text{---} \times 414$$

$$= \boxed{53} \times 664 + \boxed{-85} \times 414$$

Ex: converting numbers to different bases:

① $13_{10} = 1101_2 = D_{16}$

104_5 , 192_{10}

② $2314_5 = \boxed{334_{10}}$

$$(4\times5^0)+(1\times5^1)+(3\times5^2)+(2\times5^3) = 4+5+75+250 = 334$$

Th. Integers a, b, c such that if $\gcd(a,b)=1$ and $a \mid bc$ then $a \mid c$

In general

$a \mid bc$ (three possibilities)

- $a \mid b$
- or $a \mid c$
- or $a \nmid b$ and $a \nmid c$

$a=6$

$b=3$

$c=4$

Ex: $357_8 = ?_5 = 1424_5$

sol:

in base 10

$(7\times8^0)+(5\times8^1)+(3\times8^2)$

$= 239_{10}$

239_{10} ÷5 → 47, 4 ; 47 ÷5 → 9, 2 ; 9 ÷5 → 1, 4

Proof:

Since $\gcd(a,b) = 1$

there exist integers $x, y \in \mathbb{Z}$ such that

$$ax + by = 1 \quad \text{(linear combination)}$$

multiply by c

$$\underbrace{acx}_{\text{divisible by } a} + \underbrace{bcy}_{\text{divisible by } a \text{ since } a \mid bc} = c$$

$\therefore a \mid acx \leftarrow$ divisible by a

$a \mid bcy \rightarrow$ since $a \mid bc$

if a divides these, it also divides their sum $\rightarrow \therefore a \mid c$

✓ *** Lemma:**

p is a prime

if $p \mid a_1 a_2 a_3 \cdots a_n$

then $p \mid a_i$ for some i $\quad 1 \le i \le k$ ← يسمى أن يكون عدد prime

$p \nmid a_1$

$p \nmid a_2$

Let $m > 0$, and a, b, c are integers,

Th. if $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod m$

Proof:

$m \mid (ac - bc)$

$m \mid c \cdot (a - b)$

So $m \nmid c$

$\therefore m \mid (a - b)$

(in general) $ac \equiv bc \pmod m$

↳ can't cancel c from both sides. unless $\gcd(c, m) = 1$.

c and m relatively Prime. ↑ Logic

Ex①

$m = 4$, $c = 2$, $a = 7$, $b = 5$

$14 = 10 \pmod 4$

$7 \times 2 \equiv 5 \times 2 \pmod 4$

$7 \not\equiv 5 \pmod 4$

Ex②

$m = 5$, $c = 2$, $a = 7$, $b = 2$

$14 \equiv 4 \pmod 5$

$7 \times 2 = 2 \times 2 \pmod 5$

$7 \equiv 2 \pmod 5$

Th. if $\gcd(a,m)=1$
then there exist a unique integer $a' < m$ such that
$a\,a' \equiv 1 \mod m$

a' ↓ inverse of a in modulo m.

Proof:

$\gcd(a,m)=1$

exist integer $x,y \in \mathbb{Z}$

$\ni ax+my=1$

$ax \bmod m + my \bmod m \equiv 1 \bmod m$ (my mod m = 0)

$ax \bmod m \equiv 1 \bmod m$

$ax \equiv 1 \bmod m$

x ↓ inverse of a in modulo m.

Ex: what is the inverse of 4 in modulo 7 (نريد) $= 2$

Ex: (بسيط) modulo 7

a	1	2	3	4	5	6
inverse of a	1	4	5	2	3	6

Ex: modulo 8

a	1	2	3	4	5	6	7
inverse of a	1	–	3	–	5	–	7

البسب لأننا نجد لكل a معكوس لأن 8 ليست prime number أيضا
لو كان m prime فسنجد معكوس لكل a.

Solve the equation:

$22x \equiv 5 \bmod 51$

Find x that satisfy above eq.

① Eq. has solution since 22 and 51 are relatively prime.

② compute inverse of 22 in modulo 51:

- gcd of 51 and 22 using Eucliden Algorithm.
- express gcd as linear combination of 51 and 22.

Euclidean Alg.

$51 = \boxed{2} \times 22 + \boxed{7}$

$22 = \boxed{3} \times 7 + \boxed{1}$

$\gcd(51, 22) = 1$

$= 22 - 3 \times 7$

$= 22 - 3 \times (51 - 2 \times 22)$

$= -3 \times 51 + 7 \times 22$

inverse of 22 in modulo 51

then, multiply both sides by 7:

$7 \times 22x \equiv 7 \times 5 \bmod 5$

$x \equiv 35 \bmod 51$ (unique solution)

General Solution $x = 35 + 51k$ $k \in \mathbb{Z}$

$x = 35$

$= 86$

$= 137$

$= \vdots$

Solve the equation:

$$22x + 12 \equiv 5 \bmod 51$$

sol:

$$22x \equiv 5 - 12 \bmod 51$$
$$\equiv -7 \bmod 51$$
$$\equiv 44 \bmod 51$$

$$22x \equiv 44 \bmod 51$$

relatively prime

Recall 7 is inverse of 22 in modulo 51:

$$7 \times 22x \equiv 44 \times 7 \bmod 51$$

$$x \equiv 308 \bmod 51$$
$$\equiv 2 \bmod 51$$

(unique solution)

(General solution) $x = 2 + 51k \quad k \in \mathbb{Z}$

Ex: solve the equation:

$$4x^2 \equiv 3 \bmod 9$$

sol:

- Either we have 2 solutions or no solution.
- we may have solution since 4 and 9 are relatively prime.

Find the inverse of 4 in modulo 9:

$$9 = \boxed{2} \times 4 + \boxed{1}$$

$$\gcd(9,4) = 1$$
$$= 9 - 2 \times 4$$

-2 is inverse of 4 in mod 9

$-2 + 9$

-2 is also 7 in mod 9

$7 \times 4x^2 \equiv 7 \times 3 \mod 9$

$x^2 \equiv 21 \mod 9$

$\equiv 3 \mod 9$

no solution for x, because we can't find 3 in

تأكد أن 3 بتطلع

x	x^2	$x^2 \bmod 9$
1	1	1
2	4	4
3	9 –	0 –
4	16	7
5	25	7
6	36 –	0 –
7	49	4
8	64	1

نتوقف إلى أقل
من 9 لأننا لو أكملنا
الحلول سوف تتكرر فلن
يكون منها فائدة.

Chinese Remainder Theorem (CRT)

Given n equations

find a unique solution that satisfies them all.

$x \equiv 2 \mod 5$ $x = 2, 7, 12, 17, 22, 27, 32, \ldots$

$x \equiv 3 \mod 6$ $x = 3, 9, 15, 21, 27, 33, \ldots$

$x \equiv 2 \mod 5$ $x = 2, 7, 12, 17, 22, 27, 32, \ldots$

$x \equiv 3 \mod 10$ $x = 3, 13, 23, 33, \ldots$

No solution, because there is no common solution.

∴ Chinese Remainder Theorem needs to work only if mod values are pairwise relatively prime.

* If $m_1, m_2, m_3, \ldots, m_k$ are pairwise relatively prime, then

$x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$\vdots$

$x \equiv a_k \mod m_k$

has a unique solution $\ni 0 \leq x < m_1 \cdot m_2 \cdots m_k$.

Solving CRT

(1) check that $\gcd(m_i, m_j) = 1 \quad \forall i \neq j$ (pairwise relatively prime)

(2) Let $m = m_1 \times m_2 \times \cdots \times m_k$

(3) $M_1 = m/m_1$

$M_2 = m/m_2$

$\vdots$

$M_k = m/m_k$

(4) $x \equiv (a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_k M_k y_k) \bmod m$

$M_1 y_1 \equiv 1 \bmod m_1$ so y_1 is the inverse of M_1 in mod m

$M_2 y_2 \equiv 1 \bmod m_2$

$M_k y_k \equiv 1 \bmod m_k$

Ex// solve

$x \equiv 3 \bmod 5$

$x \equiv 2 \bmod 7$

$x \equiv 4 \bmod 8$

sol//

(1) 5, 7, 8 are pairwise relatively prime.

(2) $m = 5 \times 7 \times 8 = 280$

(3) $M_1 = m/m_1 = 280/5 = 56$

$M_2 = 40$

$M_3 = 35$

(4) $x \equiv (3 \times 56 y_1 + 2 \times 40 y_2 + 4 \times 35 y_3) \bmod 280$

for y_1 we solve $56 y_1 \equiv 1 \bmod 5$

solve $40 y_2 \equiv 1 \bmod 7$

solve $35 y_3 \equiv 1 \bmod 8$

$\gcd(56, 5)$

$56 = 11 \times 5 + 1$

$1 = 1 \times 56 - 11 \times 5$

$y_1 = 1$

$\gcd(40, 7)$

$40 = 5 \times 7 + 5$

$7 = 1 \times 5 + 2$

$5 = 2 \times 2 + 1$

$1 = 5 - 2 \times 2$

$= 5 - 2 \times (7 - 1 \times 5)$

$= -2 \times 7 + 3 \times 5$

$= -2 \times 7 + 3 \times (40 - 5 \times 7)$

$= 3 \times 40 - 17 \times 7$

$= y_2$ (inverse)

$\gcd(35, 8)$

$35 = 4 \times 8 + 3$

$8 = 2 \times 3 + 2$

$3 = 1 \times 2 + 1$

$1 = 3 - 1 \times 2$

$= 3 - 1 \times (8 - 2 \times 3)$

$= -1 \times 8 + 3 \times 3$

$= -1 \times 8 + 3 \times (35 - 4 \times 8)$

$= 3 \times 35 - 13 \times 8$

$= y_3$

$x \equiv (3 \times 56 \times 1 + 2 \times 40 \times 3 + 4 \times 35 \times 3) \bmod 280$

$\equiv 828 \bmod 280$

$\equiv 268$ (unique solution) (لأنه كان الحل عندنا واحد)

general solution → $x = 268 + 280K$ $K \in \mathbb{Z}$

Fermat's Little Theorem

* if p is prime. and $p \nmid a$, then

$$a^{p-1} \equiv 1 \bmod p$$

or

$$a^p \equiv a \bmod p$$

Ex: $10^{12} \equiv 1 \bmod 13$

$50^{96} \equiv 1 \bmod 97$

$\Rightarrow 50^{960} \equiv 1 \bmod 97$

(لأننا لو رفعنا الطرفين لن يؤثر شيء ($1 = 1^{960}$ لن تتغير))

* calculate:

$50^{1000} \bmod 97 = ? = 50^{40} \bmod 97$

$= (50^{960} \times 50^{40}) \bmod 97$ ($50^{960} = 1$)

$= (50^{32} \times 50^{8}) \bmod 97$

$\equiv 1 \bmod 97$

$50^{40} \bmod 97$

$50 \bmod 97$

$50^2 = 2500 \equiv 75 \bmod 97$

$50^4 \equiv 75^2 \bmod 97 \rightarrow \equiv 96 \bmod 97$

$50^8 \equiv 96^2 \bmod 97$

$\equiv 1 \bmod 97$

$50^{16} \bmod 97 \equiv 1^2 \bmod 97$

$50^{32} \bmod 97 = 1 \bmod 97$

Ex: $p = 19$, solve $12^{100} \bmod 19$

Sol:

$12 \equiv 12 \bmod 19$

$12^2 = 144 \equiv 11 \bmod 19$

$12^4 \equiv 11^2 \bmod 19$

$\equiv 7 \bmod 19$

$12^8 \equiv 7^2 \bmod 19$

$\equiv 11 \bmod 19$

$(12^8)^5 \equiv 1^5 \bmod 19$

$12^{90} \equiv 1 \bmod 19$

$12^{100} \equiv 12^{90} \times 12^{10} \bmod 19$ ($12^{90} = 1$)

$\equiv 12^8 \times 12^2 \bmod 19$

$\equiv 11 \times 11 \bmod 19$

$\equiv 7 \bmod 19$

---

* Random good Questions about this part of the course:

1) Calculate the value of $\sum_{k=0}^{n} \prod_{i=0}^{k} 3$.

Sol:

$$= \sum_{k=0}^{n} 3^{k+1} \Rightarrow = \sum_{k=0}^{n} 3^k \cdot 3 \Rightarrow = 3 \sum_{k=0}^{n} 3^k \Rightarrow = 3\left(\frac{3^{n+1} - 1}{2}\right)$$

Project

- solving quadratic congruence eq.:

$4a(ax^2+bx+c) \equiv 0 \mod p$ (we can write this expression like this?)

inputs

check: ① $p \nmid a$

② p odd prime.

outputs: $x = \_\_\_$, $x = \_\_\_$ } two solutions

or

"No solution"

$\Rightarrow y^2 \equiv d \mod p$

proving this expression:

$4a^2x^2+4abx+4ac \equiv 0 \mod p$ (+b^2, +b^2)

$(2ax+b)^2+4ac \equiv b^2 \mod p$

$= 4a^2x^2+4axb+b^2$

$(2ax+b)^2 \equiv b^2-4ac \mod p$

$2ax+b = y$, $b^2-4ac = d$

$y^2 \equiv d \mod p$

$d=0$? $d \neq 0$?

$y^2 \equiv 0 \mod p$

trivial

$y \equiv 0 \mod p$

$y^2 \equiv d \mod p$

$p \nmid d$

Fermat

$d^{p-1} \equiv 1 \mod p$

$\equiv 1^2 \mod p$

$d^{\frac{p-1}{2}} \equiv 1 \mod p$

we have solution

$d^{\frac{p-1}{2}} \equiv -1 \mod p$

No solution

$$\underbrace{(2ax+b)^2}_{y} \equiv \underbrace{b^2-4ac}_{d} \bmod p$$

Solution is $y^2 \equiv \alpha^2 \bmod p$

$y \equiv \begin{matrix}+\alpha \\ -\alpha\end{matrix} \bmod p$

Find $\alpha \in \mathbb{Z}_p = \{0,1,2,\dots,p-1\} \ni \alpha^2 \equiv d \bmod p$:

Alg.

$y^2 \equiv d \bmod p$
$\equiv \alpha^2 \bmod p$

```
k ← 0
while(d+pk not perfect square)
    α ← √(d+pk)

return α
```

$y^2 = (2ax+b)^2 \equiv \alpha^2 \bmod p$

$2ax+b \equiv \pm\alpha \bmod p$

$x \equiv \left(\dfrac{-b\pm\alpha}{2a}\right) \bmod p$

$\equiv \left((-b\pm\alpha) \times \text{inverse of } 2a \text{ in modulo } p\right) \bmod p$

Ex: $15x^2+19x+6 \equiv 0 \bmod 11$

Sol:

$b^2-4ac \equiv 1^2 \bmod 11$

$\alpha = 1$
$\alpha = -1$

$x \equiv \dfrac{-19\pm 1}{2\times 15} \bmod 11$

- أسوي هذه الحركة حتى لو كان ناتج الكسر انتجر ناعبر
* أحتاج إني أطلع معكوس 30 (inverse) عشان أتخلص من الكسر.

ارفعها إلى أن تصل للموجب.

$\equiv \dfrac{-18^{+4}}{30} \bmod 11 \equiv 4 \bmod 11 \times \text{inverse of } 30 \text{ in mod } 11$

$\equiv 4\times 7 \bmod 11$ (28)

$\equiv 6 \bmod 11$

ونفس الفكرة كذلك ل

$\equiv \dfrac{-20^{+2}}{30} \bmod 11 \rightarrow \equiv 14 \bmod 11$ (2x7)

$\equiv 3 \bmod 11$

inverse of 30 in mod 11 $\equiv -4$

$30 = \boxed{2} \times 11 + \boxed{8} \equiv 7$

$11 = \boxed{1} \times 8 + \boxed{3}$

$8 = \boxed{2} \times 3 + \boxed{2}$

$3 = \boxed{1} \times 2 + \boxed{1}$

$1 = 1 \cdot 3 - 1 \cdot 2$

$= 1 \cdot 3 - 1(8 - 2 \cdot 3)$

$= -1 \cdot 8 + 3 \cdot 3$

$= -1 \cdot 8 + 3(1 \cdot 11 - 1 \cdot 8)$

$= 3 \cdot 11 - 4 \cdot 8$

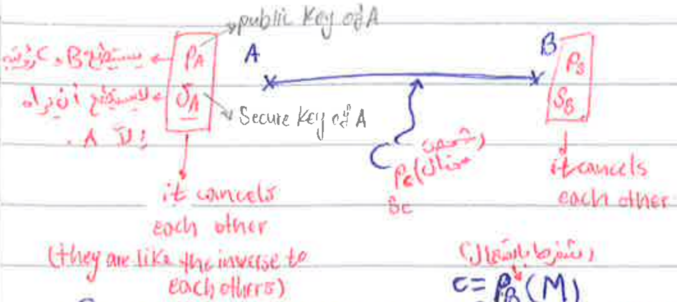
$= 3 \cdot 11 - 4(1 \cdot 30 - 2 \cdot 11)$

$= -4 \cdot 30 + 11 \cdot 11$

$=$

* RSA Cryptosystem : (inverse & chinese & Fermat تعتمد و مبنية على)

أحد تطبيقات → Public Key Cryptosystem.



M = original message.
C = Cypher message

① secure messaging $A \rightarrow B$
- $C = P_B(M)$ (تشفير باستعمال)
- B reads $M = S_B(C)$ (يستطيع قراءتها B عن طريق)

(التأكد من جاءتك الرسالة)

② Authetication : (التوثيق)

A sends $C = S_A(P_B(M))$ — يرسل A باستخدام S_A و P_B

B reads $M = P_A(S_B(C))$ — ويقرأ B 〃 P_A و S_B

RSA (تطبيقياً) : (الي فوق كان نظرياً)

① pick two large primes p, q

② $n = p \times q$

③ pick e (public key) ∋

$\gcd(e, (p-1)\cdot(q-1)) = 1$

④ Calculate d (secure key) ∋

$de \equiv 1 \bmod (p-1)\cdot(q-1)$

⑤ $C = M^e \bmod n$ (التشفير الرسالة)

⑥ $M = C^d \bmod n$ (القراءة الرسالة)

Ex: Let $p = 43$

$q = 59$

Sol:

$n = 43 \times 59 = 2537$

$(p-1)(q-1) = 2436$

Pick $e = 13$ (relatively prime — أي قيمة لم يكن لها قواسم مشتركة)

$\gcd(13, 2436) = 1$

want $de \equiv 1 \bmod 2436$

$\Rightarrow d = 937$

* قسمناها بهذه الطريقة لأننا نحتاج إلى رقم مساوي لعدد خانات الـ n لكي يخرج معنا ناتج وحيد لعملية الـ mod.

$M = \text{"STOP"} = \underbrace{\overline{18}\,\overline{19}}_{M_1}\,\underbrace{\overline{14}\,\overline{15}}_{M_2}$ (S, T, O, P)

(وضعنا تشفير من عندنا للحروف)

A 01
B 02
C 03
⋮
Z 26

$C_1 = M_1^e \bmod n$

$= 1819^{13} \bmod 2537$

$= 2081$

$C_2 = M_2^e \bmod n$

$= 1415^{13} \bmod 2537$

$= 2182$

$M_1 = C_1^d \bmod n$

$= 2081^{937} \bmod 2537$

$= 1819$

$M_2 = C_2^d \bmod n$

$= 2182^{937} \bmod 2537$

$= 1415$

Methods of Proof

- Direct Proof ($p \to q$)
- Indirect Proof ($\neg q \to \neg p$)
- Proof by contradiction ($\neg p \to F$)
- Proof by cases
- Induction
- counter example

الإثبات يتم على الصورة

hypothesis: $p \to q$ → conclusion

if p then q

Proof by cases:

$p = p_1 \vee p_2 \vee p_3 \vee \dots \vee p_n$

$p \to q \iff (p_1 \to q) \vee (p_2 \to q) \vee \dots \vee (p_n \to q)$

(Direct proof على الطريقة)

Ex: if n is odd then n^2 is odd

sol:

Proof:

Let $n = 2k+1$ for some $k \in \mathbb{Z}$

$$n^2 = (2k+1)^2$$
$$= 4k^2 + 4k + 1$$
$$= 2(2k^2 + 2k) + 1$$

($2k^2+2k$ integer)

$$= \text{odd}$$

* لسبب لإنسان قد تضطر لاستعمال Indirect Proof بسبب أنك لا تستطيع استعمال Direct Proof.

(Indirect Proof على الطريقة)

Ex: if $3n+2$ is odd then n is odd

sol:

Proof: * if you try to use direct proof, you will get unuseful answer.

Let $3n+2 = 2k+1$ $\quad k \in \mathbb{Z}$

$$n = \frac{2k-1}{3}$$

sol

* let's try to Prove by Indirect proof:

Proof: $\neg q \to \neg p$

Assume n is even ($\neg q$)

Let $n = 2k$ $\quad k \in \mathbb{Z}$

$3n+2 = 3(2k)+2$

$= 6k+2$

$= 2(3k+1) = \text{even}$ ($\neg p$)

$\neg q \to \neg p \iff p \to q$

(Indirect proof)

Ex: if n^2 even then n is even

Sol:

p $\quad$ q

Proof: when we try to use direct proof, we will get unuseful answer.

Let $n^2 = 2k \qquad k \in \mathbb{Z}$

$n = \sqrt{2k}$ ←

Proof (By Indirect proof)

Assume n is odd

$\neg q$

Let $n = 2k+1 \qquad k \in \mathbb{Z}$

then $n^2 = (2k+1)^2$

$= 4k^2 + 4k + 1$

$= 2(2k^2 + 2k) + 1$ } $\neg p$

$=$ odd

(proof by contradiction)

Ex: Show $\sqrt{2}$ is irrational

Sol:

Proof:

Assume $\sqrt{2}$ is rational

$\neg p$

(حيث أننا افترضنا x و y على أبسط صورة كسر ممكنة)

so, let $\sqrt{2} = \frac{x}{y} \qquad x, y \in \mathbb{Z} \ni \gcd(x,y) = 1$

↑ contradicts

$2 = \frac{x^2}{y^2}$ or $x^2 = 2y^2 =$ even

x is even

Let $x = 2k \qquad k \in \mathbb{Z}$

$x^2 = (2k)^2 = 2y^2$

$y^2 = 2k^2 =$ even $\Rightarrow$ y is even

so, we have a contradiction

$\therefore \sqrt{2}$ is irrational.

Ex: Show there are infinite # of primes.

Sol: **Proof.**

Assume # primes is finite. ($\neg p$)

Let primes be: $p_1, p_2, p_3, \cdots, p_n$ (Largest prime)

* Now, we try to find a prime number larger than p_n

Let $x = (p_1 \times p_2 \times p_3 \times \cdots \times p_n) + 1$

هنا composite لأننا نستطيع تحليلها على أنها primes.

$p_1 \nmid x$

$p_2 \nmid x$

$p_3 \nmid x$

$\vdots$

$p_n \nmid x$

* إذا كان x (composite) فيجب على الأقل أن يقسم prime number واحد على الأقل ، ولكنه لم يقسم أياً من primes

$\Rightarrow$ x is prim $> p_n$

(by cases)

Ex: Show that the product of three consecutive integers is divisible by 3.

Sol: **Proof.**

show $3 \mid x \cdot (x+1) \cdot (x+2)$

- case 1: x is divisible by 3
  - $3 \mid x$
  - $\therefore 3 \mid x(x+1)(x+2)$ (a|b then a|bc)
- case 2: we have reminder of 1 when divides x by 3
  - $3 \mid (x+2)$
  - $\therefore 3 \mid (x+2)(x+1)x$
- case 3: we have reminder of 2 when dividing x by 3
  - $3 \mid (x+1)$
  - $\therefore 3 \mid (x+1)(x+2)x$

(by cases)

Ex Show that a number ending with 2 cannot be a perfect square.

حل:

perfect square: 1, 4, 9, 16, 25, ...

نقدر نكتب أي رقم بهذه الطريقة.

Let $n = 10k + \ell$ ← $k \geq 0$, $\ell \in \{0, 1, 2, \dots, 9\}$

$$n^2 = (10k+\ell)^2$$
$$= 100k^2 + 20k\ell + \ell^2$$
$$= 10(10k^2 + 2k\ell) + \ell^2$$

هذه بتكون من مضاعفات 10 فليست منه احتمالنا لأن آحادها ليست 2

نزيهم

case $\ell = 0$

n^2 ends with 0

case $\ell = 1$

n^2 ends with 1

∴ doesn't possible that a number ending with 2 can be a perfect square.

ℓ	ℓ^2	n^2 ends in ← خانة الآحاد
0	0	0
1	1	1
2	4	4
3	9	9
4	16	6
5	25	5
6	36	6
7	49	9
8	64	4
9	81	1

(مثال مناقض)

Counter example :

Ex: "All primes are odd integers"

sol: 2 is an even prime

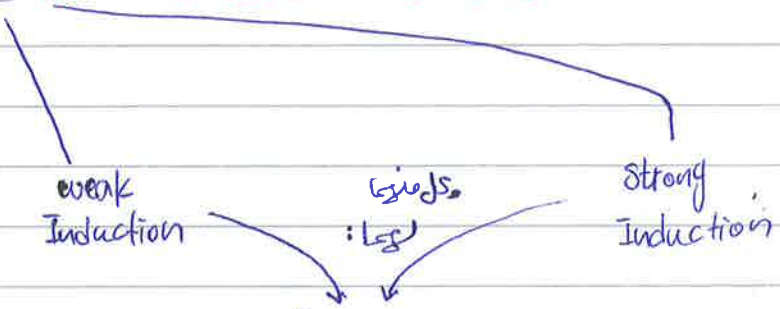
Ex: if a|bc then a|b or a|c

sol:

a=12	12|48
b=3	12∤3
c=16	12∤16

if a|b then a|bc : ليست العكس نفسها بالعكس.

Induction: (يستعمل لتوثيق النظرية وليس لإثباتها أو اشتقاقها)



Weak Induction:

$$[P(1) \wedge P(n) \rightarrow P(n+1)]$$

(النتيجة التي نريد الوصول إليها) $\rightarrow \forall n\ P(n)$

Ex: Show that "$n! > 2^n$" for all $n \geq 4$ ($P(n)$=)

sol:

Base case (n=4):

$4! > 2^4 \Rightarrow 24 > 16$ ∴ True.

Inductive case:

we Assume that P(n) and we will prove that P(n+1) is true.

$n! > 2^n \Rightarrow (n+1)\cdot n! > 2^n \cdot (n+1)$ based on induction hypothesis

$(n+1)! > 2^n \cdot 2$

$> 2^{n+1}$

∴ P(n+1) is true.

(week)

Ex: Show that

$P(n) = \text{"} \sum_{k=1}^{n} k = \frac{1}{2} n \times (n+1) \text{"}$

Sol:

Base case ($n = 1$)

LHS $P(1) = \sum_{k=1}^{1} k = 1$

RHS $P(1) = \frac{1}{2} \times 1 \times 2 = 1$

$=$

Base case is True.

- Inductive case: → [$P(1) \wedge P(n) \rightarrow P(n+1)$] (تحاول أن تصل إلى هذه)

Assume $P(n)$ is True for some n. We show it's true for $P(n+1)$.

LHS $P(n+1) = \sum_{k=1}^{n+1} k$

$= \left(\sum_{k=1}^{n} k\right) + (n+1)$

$= \frac{1}{2} n \times (n+1)$ based on induction hypothesis

$= (n+1)\left[\frac{n}{2} + 1\right]$

$= \frac{1}{2}(n+1)(n+2)$

$=$ RHS $P(n+1)$ ✓

$\therefore [P(1) \wedge P(n) \rightarrow P(n+1)]$ (توصلنا إليها عن طريق)

إذا تنطبق → $\forall n \; P(n)$

(weak)

Ex: Show that

$$P(n) = \sum_{k=m}^{n} k = \frac{1}{2}\left[n(n+1) - m(m-1)\right]$$

Sol:

Base case ($n = m$ أصغر قيمة لـ n)

$$\text{LHS } P(m) = \sum_{k=m}^{m} k = m$$

$$\text{RHS } P(m) = \frac{1}{2}\left[m(m+1) - m(m-1)\right]$$

$$= \frac{m}{2}\left[m+1 - (m-1)\right]$$

$$= \frac{m}{2} \times 2 = m$$

$\therefore$ Base case True.

Inductive case:

Assume $P(n)$ is True for some n. We show it's True for $P(n+1)$.

$$\text{LHS } P(n+1) = \sum_{k=m}^{n+1} k$$

$$= \left(\sum_{k=m}^{n} k\right) + (n+1)$$

$$= \frac{1}{2}\left[n(n+1) - m(m-1)\right]$$ based on induction hypothesis

$$= \frac{1}{2}\left[n(n+1) - m(m-1) + 2(n+1)\right]$$

$$= \frac{1}{2}\left[(n+1)(n+2) - m(m-1)\right]$$

$$= \text{RHS } P(n+1)$$

Ex: for $n \geq 1$, Show that $3 \mid (n^3 - n)$.

Sol:

Base case ($n=1$)

$3 \mid (1^3 - 1)$

So it's true.

Inductive case

Assume it's true for some n. we show it's true for $n+1$.

$$(n+1)^3 - (n+1)$$
$$= (n^3 + 3n^2 + 3n + 1) - (n+1)$$
$$= (n^3 - n) + 3(n^2 + n)$$

$(n^3 - n)$: divisible by 3 based on induction hypothesis

$3(n^2+n)$: multiple of 3

∴ منها أنه جميعاً تقسم 3 فإذاً المجموع يقسم الـ 3.

$(a \mid b \ \& \ a \mid c) \therefore a \mid (b+c)$

$\therefore 3 \mid ((n+1)^3 - (n+1))$

Strong Induction :

Base case $P(1)$ is true.

Inductive case:

Assume $P(1) \wedge P(2) \wedge P(3) \wedge \dots \wedge P(n)$ all are true.

then we show $P(n+1)$ is true.

(strong)

Ex: Show that for all $n \geq 2$ can be written as product of primes.

Sol:

Base case ($n=2$)

2 is prime, so it's true.

Inductive case

Assume all integers

$2, 3, 4, 5, 6, \ldots, n$

can be expressed using primes.

we show it's true for $n+1$.

$n+1$

case 1: $n+1$ is prime (Done)

case 2: $n+1$ is composite

$\exists$ two integers $a \times b$

where $1 < a \leq b < n+1$

$\therefore n+1 = a \times b$

True based on induction hypothesis

True based on induction hypothesis

$\therefore n+1$ can be written using product of primes.

(strong)

Ex: Show all numbers ≥ 8 can be written using sum of 3s and 5s.

like this

$9 = 3+3$

$10 = 5+5$

$11 = 3+3+5$

$12 = 3+3+3+3$

$13 = 3+5+5$

⋮

Sol:

Base case ($n = 8$)

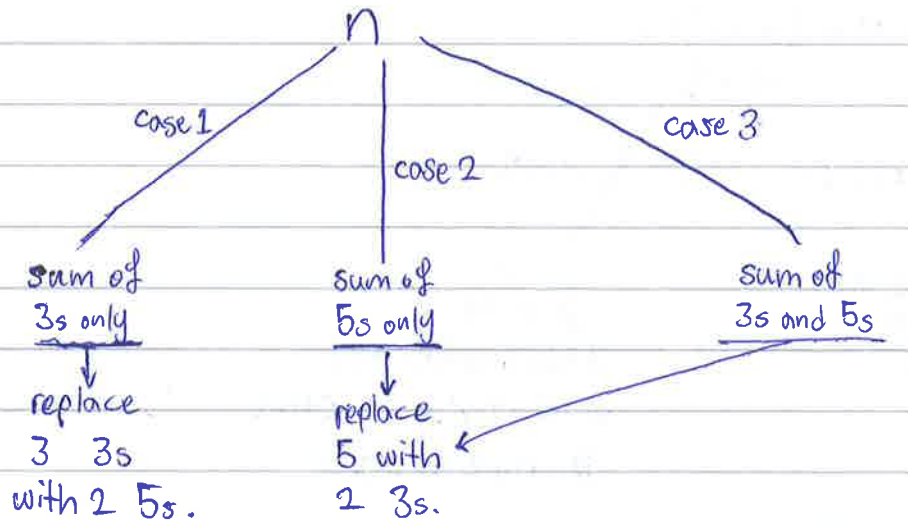
$8 = 3+5$ so it's true.

Inductive case

Assume it's True for

$8, 9, 10, 11, \ldots, n$

we show it's True for $n+1$.



Combinatorics

it's about Counting.

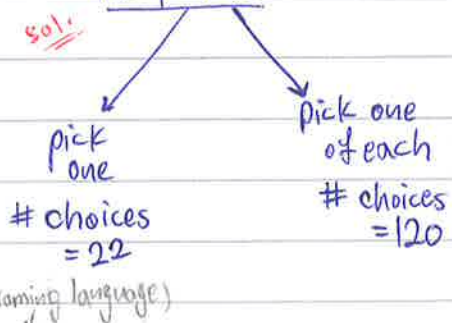
Sum rule: Do either task = $|T_1| + |T_2|$

Product rule: Do both tasks = $|T_1| \times |T_2|$

Two tasks T_1, T_2

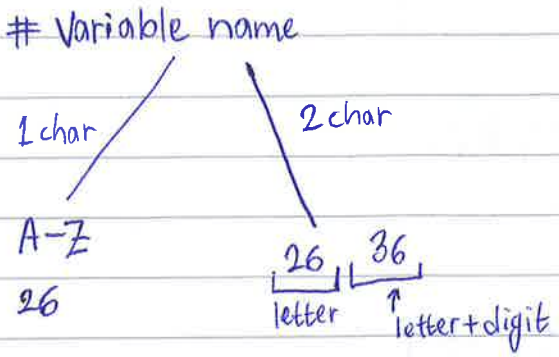
Ex: 10 pens
12 pencils

sol:



Ex: PL (programming language) allows varible names of up to 2 characters.
First characters is letter, 2nd character is alphanumeric.
Letters are case insensitive. → AB, Ab, aB, ab } same
How many varible names?

sol:



varible names
$= 26 + 26 \times 36$
$= 962$

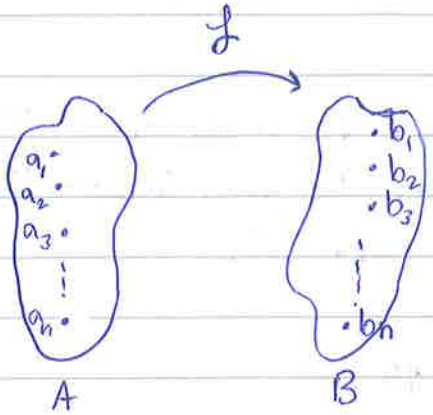
Ex: $f: A \to B$

How many functions f can we have?

Sol:

Let $|A| = n$

$|B| = m$



each $a_i \in A$ has m choices

$m \times m \times m \times \cdots \times m$

$= m^n$

Over Counting :

Ex: How many bit strings (binary) of length 8 that has either 1 in leftmost bit or ends with 00.

Sol:

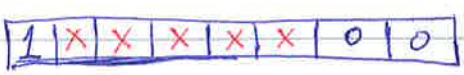
0 or 1

$= 2^7$

or

$= 2^6$

Common



$= 2^5$

$= 2^7 + 2^6 - 2^5 = 160$

Pegionhole Principle :

Th. if we place $k+1$ objects in k boxes,
then there is a box with more than one object.

Th. if we place N in k boxes,
then there is a box with at least $\lceil \frac{N}{k} \rceil$ objects. (General form of the principle)

Ex. 10 black socks
10 white "
10 brown "
How many socks shall I pick to guarantee two socks of same color?

sol:

pick smallest N
socks $\ni$
$\lceil \frac{N}{3} \rceil = 2$ → عدد الجوارب الي أريد اختيارها

(3 ← عدد الألوان)

Ex. Given numbers $\{1, 2, 3, 4, \cdots, 25\}$.
show that if you pick any 14 numbers from above set without repetition, there are two which sums 26.

sol:

1	2	3	4	5	6	7	8	9	10	11	12	13
25	24	23	22	21	20	19	18	17	16	15	14	

* نلاحظ أننا حاولنا نشوف أسوء سيناريو بحيث نختار أعداد بالشكل.
ولكن باقي رقم واحد ما اخترنا لأنه قايل
اختر 14 رقم وليس 13،
والرقم الأخير بيكون غصب يتجمع مع شيء وينتج = 26.

Permutation – ordered arrangment $P(n,r) = n(n-1)(n-2)\cdots(n-r+1) = \boxed{\frac{n!}{(n-r)!}}$

Combination – unordered selection

$$C(n,r) = \binom{n}{r} = \frac{P(n,r)}{r!} = \boxed{\frac{n!}{r! \times (n-r)!}}$$

(Permutation)

Ex: 3 boys.
2 prizes.

Sol:

$P(3,2) = 6$

Ahmad, Omar, Ali (ترتيب)

1st prize	2nd prize	
Ahmad	Omar	✓
Omar	Ahmad	✓
Ahmad	Ali	✓
Ali	Ahmad	✓
Omar	Ali	✓
Ali	Omar	✓

(combination)

Ex: ~~3 balls~~
pick 2.

Sol:

$C(3,2) = 3$

(توفيق)

White ball	blue ball	red ball
X	X	
X		X
	X	X

Ex: How many bit strings of length 8 that has 3 zeros.

Sol:

$$C(8,3) = \frac{8!}{3! \times 5!} = \frac{8 \times 7 \times 6}{6} = 56$$

Do, but at most 3 zeros.

$$\binom{8}{0} + \binom{8}{1} + \binom{8}{2} + \binom{8}{3}$$

No zero — 1 zero

لماذا + لأنه لا يمكن أن يكون الحالتين في نفس الوقت

$$= \sum_{k=0}^{3} \binom{8}{k}$$

Ex: 5 people

How many way to picture in group of 3.

Sol:

$P(5,3) = 5 \times 4 \times 3$

5	4	3

$= 5 \times 4 \times 3$

فكرة أخرى للحل:

اختيار 3 أشخاص من أصل 5

عدد طرق ترتيب هؤلاء الثلاثة

$\binom{5}{3} \times 3!$

إذا افترضنا أن شخصاً أراد دائماً أن يكون في كل الصور:

1	4	3

$= 12$

نشترط الشرط أن يكون موجود في كل الصور

Ex: 10 books

ways to arrange them?

Sol:

10	9	8	.....	1

$= 10!$

Ex: 10 books

4 books in Math. $4!$

3 // // CS. $3!$

3 // // Islam. $3!$

Arrange them so all books of same subjects are together.

Sol:

$= 4! \times 3! \times 3! \times 3!$

نضربهم لأن وقت اختيار كم في نفس الوقت.

M	C	I

M	I	C

I	M	C

(ترتيب المواد نفسها)

$3!$

Ex A computer system has passwords of length 6 or 7.
Each password is made up of letters (case sensitive) or numerals.
The password must have at least one numeral.

sol:

P_6 = # passwords of length = 6

$$= \sum_{k=1}^{6} \binom{6}{k} \times 52^{6-k} \times 10^{k}$$

52 < a-z, A-Z
10 < 0-9

(طريقة أخرى) $= 62^6 - 52^6$
(كل الحالات) (فقط أحرف)

password with 1 numeral.

$= 52^5 \times 10 \times \binom{6}{1}$

Password with 2 numeral.

$= 52^4 \times 10^2 \times \binom{6}{2}$

Pascal triangle

n							
0				1			
1			1		1		
2		1		2		1	= 4
3	1		3		3		1 = 8
4	1	4		6		4	1 = 16
5	1	5	10		10	5	1

k=0, k=1, k=2

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$ (مجموع كل صف)

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$ (يدل أن صفوفه Symmetric)

proof:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

$$\frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\times(n-k+1)!} \qquad (k\times(k-1)!)$$

$$\frac{n!}{(k-1)!\,(n-k)!}\left[\frac{1}{k} + \frac{1}{(n-k+1)}\right]$$

$$\frac{n-k+1+k}{k\,(n-k+1)} \Rightarrow \frac{n+1}{k\,(n-k+1)}$$

Binomial Expansion: (أضف الاستعمالات المثلث باسكال)

$a, b \in \mathbb{R}$

$n \in \mathbb{Z}^+$

$$(a+b)^n =$$

$$\sum_{k=0}^{n} \binom{n}{k} a^{n-k} \times b^k \quad \text{(أي صورة منهم عادي)}$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^k \times b^{n-k}$$

Ex: $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$

Sol:

$$(a-b)^4 = \sum_{k=0}^{4} \binom{4}{k} a^{4-k} \times (-b)^k$$

(طلعنا بالسالب)

$$= a^4 - 4a^3b + 6a^2b^2 - 4ab^3 + b^4$$

Ex: $(x^2+3y)^5$

Sol:

$$= \sum_{k=0}^{5} \binom{5}{k} (x^2)^k (3y)^{5-k}$$

$$= (3y)^5 + 5(x^2)^1(3y)^4 + 10(x^2)^2(3y)^3 + 10(x^2)^3(3y)^2 + 5(x^2)^4(3y) + (x^2)^5$$

Ex: expands $(a+b)^5$.

Sol:

$$= \sum_{k=0}^{5} \binom{5}{k} a^{5-k} b^k$$

$$= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

Ex: What's the coeff. of x^{20} in the expansion of $(3x^2 - \frac{4}{x})^{30}$.

Sol:

$$= \sum_{k=0}^{30} \binom{30}{k} (3x^2)^k \left(-\frac{4}{x}\right)^{30-k}$$

$$3^k \cdot x^{2k} \cdot (-4)^{30-k} \cdot (x)^{k-30}$$

$$3^k \cdot (-4)^{30-k} \cdot (x)^{2k+k-30}$$

$$3^k (-4)^{30-k} \cdot x^{3k-30}$$

$3k - 30 = 20$

$\Rightarrow k = \frac{50}{3}$ ← لأن k لا تكون كسرا (integer) صحيحا

so, coeff. of $x^{20} = 0$

$x^{20} = x^{3k-30}$

Ex: coeff. of x^9 in $(3x^2 - \frac{4}{x})^{30}$.

Sol:

$x^9 = x^{3k-30}$

$3k - 30 = 9$

$\Rightarrow k = \frac{39}{3} = 13$

coeff. of $x^9 = \binom{30}{13} \cdot 3^{13} \cdot (-4)^{17}$

Proof:

① $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ إذا $a=1, b=1$ في

② $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$ إذا $a=1, b=-1$ في

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$ (Binomial Expansion)

Ex: Find the coeff. of x^5y^8 in the expansion $(2x - y^2)^9$.

Sol:

$$(2x - y^2)^9 = \sum_{k=0}^{9} \binom{9}{k} (2x)^{9-k} (-y^2)^k$$

$$2^{9-k} \cdot x^{9-k} \cdot (-1)^k \cdot y^{2k}$$

$x^5 = x^{9-k}$

$9 - k = 5$

$k = 4$

$y^{2k} = y^8$

$2k = 8$

$k = 4$

* لو تأخذ أي منهما لحساب الـ k عن طريق الأس سيخرج لك نفس الناتج لـ k.

coeff. of $x^5y^8 = \binom{9}{4} \times 2^5 \times (-1)^4$

$= 32 \binom{9}{4}$

Th. Vandermonde's Identity:

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$

$m, n, r \in \mathbb{N}$ and $r \leq \min(n, m)$

Special case

$m = r = n$

$$\binom{2n}{n} = \sum_{k=0}^{n} \binom{n}{k}^2$$

Binomial Expansion:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}$$

but, $(a+b+c)^n = ?$

$(a+b+c+d+e+f)^n = ?$

Multinomial expansion:

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{n_1+n_2+\cdots+n_k=n} \frac{n!}{n_1! \times n_2! \times \cdots \times n_k!} x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$$

$k=2$

$$(x_1+x_2)^n = \sum_{n_1+n_2=n} \frac{n!}{n_1! \times n_2!} x_1^{n_1} \cdot x_2^{n_2}$$

$n_2 = n - n_1$

$$(x_1+x_2)^n = \sum_{n_1+n_2=n} \frac{n!}{n_1! \times (n-n_1)!} x_1^{n_1} \cdot x_2^{n-n_1}$$

Rewrite above using k instead of n_1:

$$(x_1+x_2)^n = \sum_{k=0}^{n} \frac{n!}{k!\,(n-k)!} x_1^{k} \cdot x_2^{n-k}$$ (Binomial expansion)

k=3

Ex: $(a+b+c)^4$

Sol:

$$= \sum_{n_1+n_2+n_3=4} \frac{4!}{n_1! \cdot n_2! \cdot n_3!} a^{n_1} \cdot b^{n_2} \cdot c^{n_3}$$

$= c^4 + 4bc^3 + 6b^2c^2 + 4b^3c$
$+ b^4 + 4ac^3 + 12abc^2 + 12ab^2c$
$+ 4ab^3 + 12a^2bc + 6a^2b^2$
$+ 4a^3c + 4a^3b + a^4$
$+ 6a^2c^2$

n_1	n_2	n_3	
0	0	4	c^4
0	1	3	bc^3
0	2	2	b^2c^2
0	3	1	b^3c
0	4	0	b^4
1	0	3	ac^3
1	1	2	abc^2
1	2	1	ab^2c
1	3	0	ab^3
2	0	2	a^2c^2
2	1	1	a^2bc
2	2	0	a^2b^2
3	0	1	a^3b
3	1	0	a^3c
4	0	0	a^4

Ex: What's the coeff. of $x^3y^4z^3$ when expanding $(x+2y+3z)^{10}$.

Sol:

$$(x+2y+3z)^{10} = \sum_{n_1+n_2+n_3=10} \frac{10!}{n_1! \times n_2! \times n_3!} x^{n_1} \cdot (2y)^{n_2} \cdot (3z)^{n_3}$$

coeff. of $x^3y^4z^3 \Rightarrow n_1=3, n_2=4, n_3=3$

$$= \frac{10!}{3! \cdot 4! \cdot 3!} 2^4 \cdot 3^3$$

Multinomial Expansion

$$(x_1+x_2+\cdots+x_k)^n$$

$$= \sum_{n_1+n_2+\cdots+n_k} \frac{n!}{n_1! \times n_2! \times \cdots \times n_k} \prod_{i=0}^{k} x_i^{n_i}$$

Ex: Expand $(x+y+z)^2$

sol:

$$(x+y+z)^2 = \sum_{n_1+n_2+n_3=2} \frac{2!}{n_1! \times n_2! \times n_3!} x^{n_1} y^{n_2} z^{n_3}$$

$$= z^2+2yz+y^2+2xz+2xy+x^2$$

n_1	n_2	n_3	
0	0	2	z^2
0	1	1	yz
0	2	0	y^2
1	0	1	xz
1	1	0	xy
2	0	0	x^2

Ex: In the expansion of $(2x+3x^2+\frac{4}{x})^6$

(a) what is the coeff. of x^5.

(b) " " " max power of x. $= x^{12}$

sol:

$$(2x+3x^2+\frac{4}{x})^6 = \sum_{n_1+n_2+n_3=6} \frac{6!}{n_1! \times n_2! \times n_3!} (2x)^{n_1} (3x^2)^{n_2} (\frac{4}{x})^{n_3}$$

$\Downarrow$

$n_3 = 6-n_1-n_2$

من طريق آخر

$$2^{n_1} 3^{n_2} 4^{n_3} x^{n_1+2n_2-n_3}$$

$$x^{n_1+2n_2-(6-n_1-n_2)}$$

$$x^{2n_1+3n_2-6}$$

نبدأ بكم

$$x^5 = x^{2n_1+3n_2-6}$$

$$2n_1+3n_2=11$$

$$0 \le n_1, n_2 \le 6$$

n_1	n_2
1	3
4	1

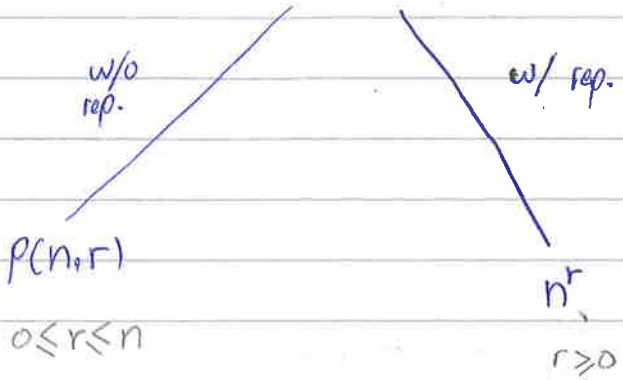
Coeff. of x^5:

$$\left(\frac{6!}{1! \times 2! \times 3!} \times 2^1 \times 3^3 \times 4^2 + \frac{6!}{4! \times 1! \times 1!} \times 2^4 \times 3^1 \times 4^1 \right)$$

Permutation and Combination with repetition

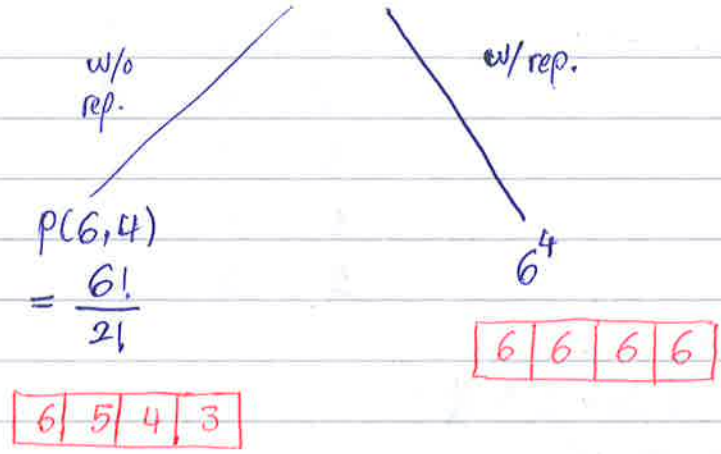
(Permutation)

① # ways to arrange r objects out of n objects.



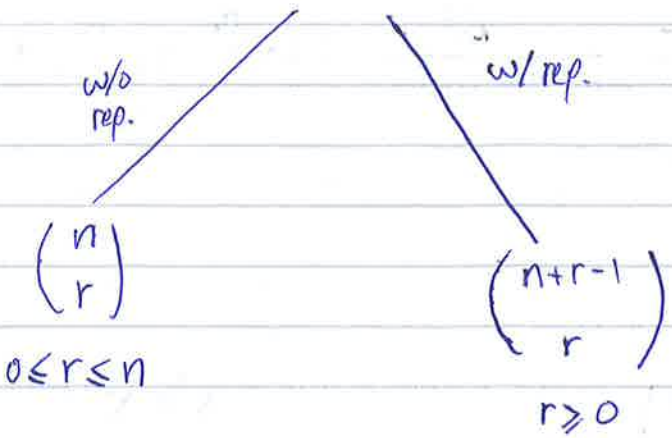
Ex: How many 4 letter words can you write using the letters: A, B, C, D, E, F.

Sol:



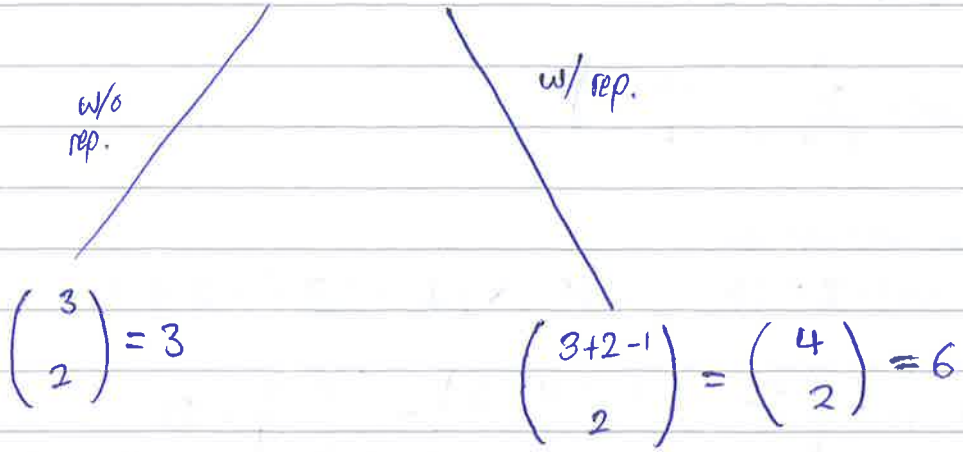
(Combination)

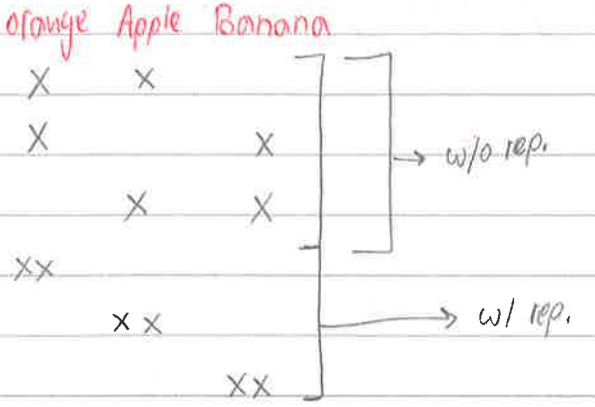
② # ways to select r objects out of n objects.



Ex: 3 different fruits. pick 2 fruits.

sol:





Ex: How many integer solutions do we have to the eq: (نفس فكرة السؤال السابق)

sol:

$$x_1 + x_2 + x_3 = 11 \quad , x_1, x_2, x_3 \geq 0$$

كأنك بقول اقسم تلات فواكه من أصل 11 فاكهة.

$$\#\text{ Solutions} = \binom{3+11-1}{11} = \binom{13}{11} = \frac{13 \times 12}{2} = 78$$

Ex: How many solutions do we have for eq:

$$x + y + z \leq 11 \quad , \quad x, y, z \in \mathbb{N}$$

sol:

\# solutions to $x+y+z=0$

\+ // // // $x+y+z=1$

\+ // // // $x+y+z=2$

⋮

\+ // // // $x+y+z=11$

so,

$$\#\text{ Solutions} = \sum_{k=0}^{11} \binom{3+k-1}{k}$$

Ex: How many solutions do we have for

$9 \leq x+y+z \leq 11$, $x,y,z \in \mathbb{N}$

Sol:

$$\#\text{solutions} = \sum_{k=9}^{11} \binom{3+k-1}{k}$$

Ex: How many solutions for

$x+y+z = 11$ ∋ $x \geq 1$, $y \geq 2$, $z \geq 4$

Sol:

$$\#\text{solutions} = \binom{3+(11-1-2-4)-1}{11-1-2-4} = \binom{6}{4} = 15$$

كيف وصلنا إلى هذا ؟

* أعدنا كتابة المعادلة :

$(x'+1)+(y'+2)+(z'+4) = 11$

∋ $x,y,z \geq 0$

$x'+y'+z' = 11-1-2-4$

$= 4$

x	y	z
1	2	8
1	3	7
1	4	6
1	5	5
1	6	4
2	2	7
2	3	6
2	4	5
2	5	4
3	2	6
3	3	5
3	4	4
4	2	5
4	3	4
5	2	4

كل الحلول الممكنة

Ex: Letters: A, B, C, D, E, F

(a) # words of length 4 (no rep.)

(b) " " " " " (w/ rep.)

(c) # words of length 6 (no rep.) such that A and B together.

(d) # Words of length 6 (no rep.) such that A and B not together.

Sol:

(a) $P(6,4)$

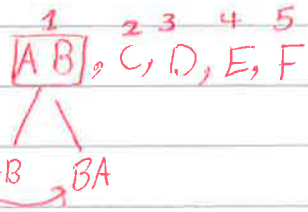
6	5	4	3

(b) 6^4

6	6	6	6

(c) $5! \times 2!$

لأننا اعتبرنا أن A&B حرف مركب واحد



(d) $6! - 5! \times 2!$

Ex: How many distinct words can you write by re-arrange the letters in the name: AZZAM.

$$\frac{5!}{2! \times 2!}$$

A Z

if we say: AZIZ

$$\frac{4!}{2!} = \frac{24}{2} = 12$$

if we say: SUCCESS

$$\frac{7!}{2! \times 3!}$$

Advanced Counting Techniques

Problem ⟶ Recursive Relation + Initial condition (Solution)

Ex: The number of bacterias double every hour. We start with 5 bacterias ($b_0 = 5$). How many do we have after 10 hours ($b_{10} = ?$) assuming all are still alive?

Sol:

let b_n = # bacterias after n hours

$b_n = 2b_{n-1}$

$b_1 = 2b_0 = 10$
$b_2 = 2b_1 = 20$
$b_3 = 2b_2 = 40$
$b_4 = 2b_3 = 80$
⋮
b_{10} = answer

Ex: A bank gives loan with interest of 11% compounded annually. Suppose you took a 100,000 Riyal loan. How much you own the bank after 5 years.

Sol:

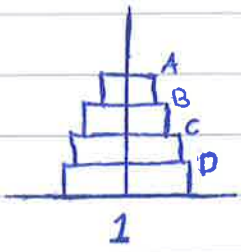
let L_n = The loan after n years

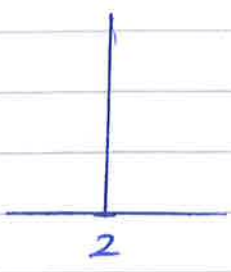
$L_n = L_{n-1} + 0.11 L_{n-1} = 1.11 L_{n-1}$

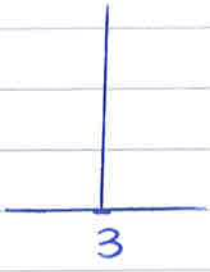
$L_0 = 100{,}000$
$L_1 = 1.11 \times 100{,}000 = 111{,}000$
$L_2 = 1.11 \times 111{,}000 = 123210$
$L_3 = 1.11 \times L_2 = \ldots$
⋮
L_5 = answer

Ex: Tower of Honai: How many moves needed to solve tower of hanoi with n disks.

Sol:

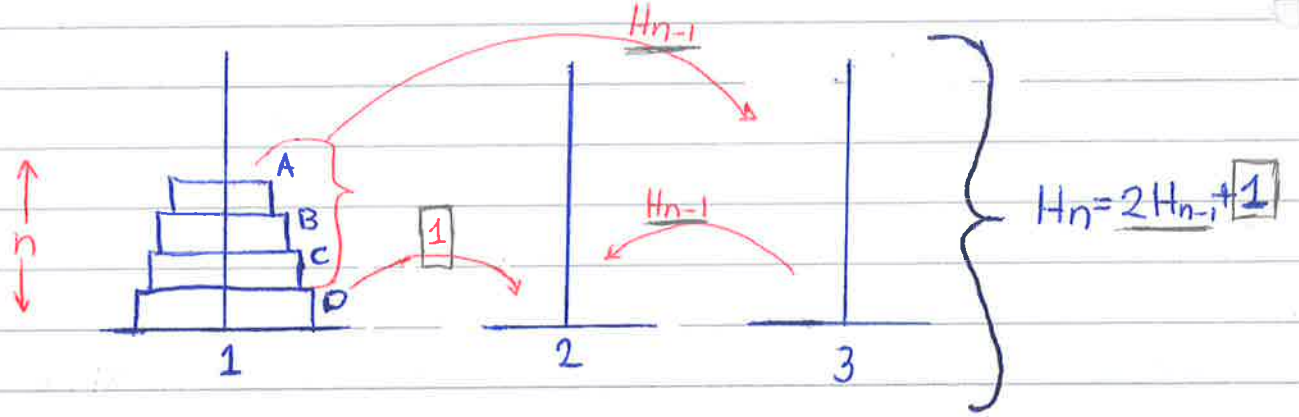






A $1 \to 3$
B $1 \to 2$
A $3 \to 2$
C $1 \to 3$
A $2 \to 1$
⋮

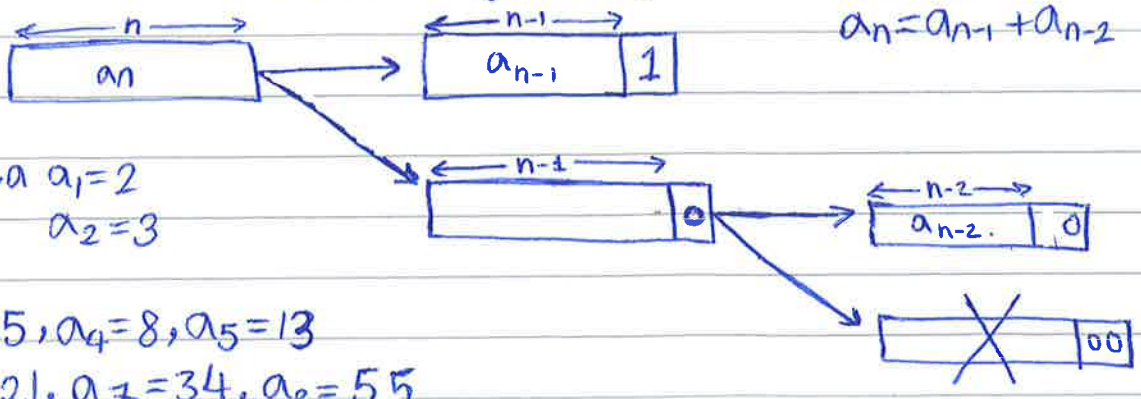
Let H_n = # moves to move all disks from 1 to 2 with n disks.



I.C. $H_1 = 1$
$H_2 = 3$
$H_3 = 7$
$H_4 = 15$

(1)
Ex: How many bit strings of length 8 that does not have two consecutive zeros.

Sol: Let a_n = # bit of strings of length n with no 00.



I.C.a $a_1 = 2$
$a_2 = 3$

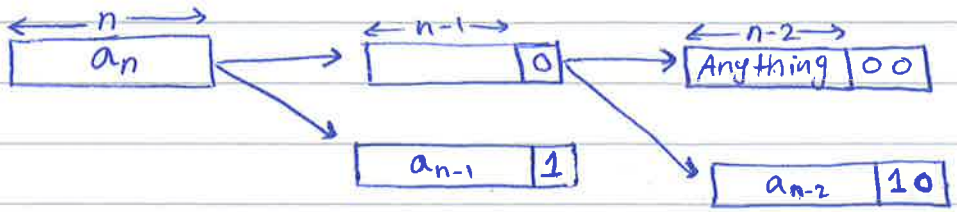
$a_3 = 5, a_4 = 8, a_5 = 13$
$a_6 = 21, a_7 = 34, a_8 = 55$

Ex: How many bit strings of length 8 that has two consecutive zeros.

Sol:

So we want a_8

Let a_n = # Bit of length n having 00



I.C. $a_1 = 0$, $a_2 = 1$

$a_n = a_{n-1} + a_{n-2} +$ (anything in n-2 bits) 2^{n-2}

$= a_{n-1} + a_{n-2} + 2^{n-2}$.

Recurrence Relation (R.R.)

$a_3 = 0 + 1 + 2^1 = 3$

$a_4 = 1 + 3 + 2^2 = 8$

$a_5 = 3 + 8 + 2^3 = 19$

$a_6 = 8 + 19 + 2^4 = 43$

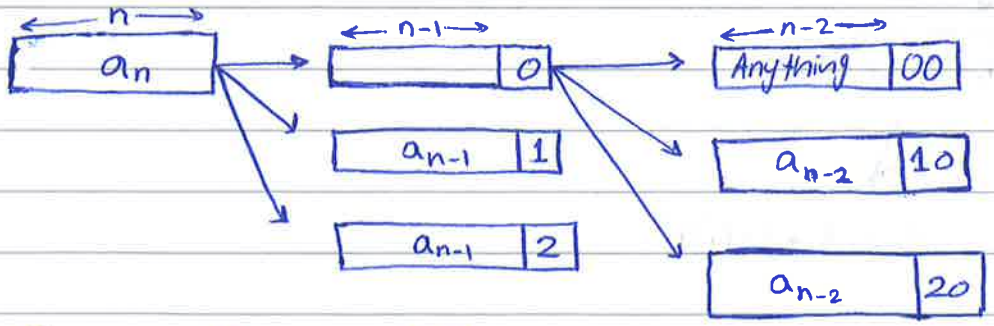
$\vdots$

a_8 = answer

Ex: How many ternary (0,1,2) string of length 8 that has two consecutive zeros.

Sol:

Let a_n = # ternary strings of length n with 00



I.C. $a_1 = 0$, $a_2 = 1$

RR $a_n = 2a_{n-1} + 2a_{n-2} + 3^{n-2}$

$a_3 = 2\times0 + 2\times1 + 3^1 = 5$

$a_4 = 2\times1 + 2\times5 + 3^2 = 21$

$\vdots$

a_8 = answer

Solving Recurrence Relations

Recurrence ال
* فكرتها تحويل المعادلة إلى معادلة لا تتطلب معطيات مسبقة.
$a_n = a_{n-1} + a_{n-2}$
لو قلنا a_{30} → فنضطر نحل كل المعادلة
بينما لو كانت المعادلة لا تحتوي قيم سابقة غير القيم الأولية فنحن نستطيع حلها بسهولة.

- Linear
  $a_n = ? a_{n-1} + ? a_{n-2} + \cdots$
  non Linear
  $a_n = a_{n-1}^2$

* قد تكون Linear وليست Homo
مثل:
$a_n = a_{n-1} + a_{n-2}^2$

- Homogeneous $a_n = a_{n-1} + a_{n-2} + a_{n-3} \cdots$
  non-homogeneous $a_n = a_{n-1} + 5$.
- Constant Coeff. → $a_n = a_{n-1} + 5a_{n-2}$
  non-constant coeff $a_n = n a_{n-1}$
- Degree = 2.
  degree (3) → $a_n = a_{n-2} + 5a_{n-3}$..
  $a_n = a_{n-5}$ (Degree 5)

$a_n = c_1 a_{n-1} + c_2 a_{n-2}$
↓ ↓
constant
⇓
Characteristic eq.
$r^2 - c_1 r - c_2 = 0$ (Quadratic equation)

two different roots (r_1, r_2)
$r_1 \neq r_2$
↓
$a_n = d_1 r_1^n + d_2 r_2^n$

same root
$r_1 = r_2 = r$
↓
$a_n = (d_1 + d_2 n) r^n$

Ex: Go to example (1).

Sol.

$$a_n = a_{n-1} + a_{n-2}$$

I.C. $a_1 = 2$

$a_2 = 3$

→ Char. eq.

$r^2 - r - 1 = 0$

$$\text{roots} = \frac{1 \pm \sqrt{1+4\times 1}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

← قانون الجذر

قانون الجذر:

$$x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

$$a_n = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^n + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^n$$

$a_1 = 2$, $a_2 = 3$

$$a_1 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^1 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^1 = 2$$

$$a_2 = \alpha_1 \left(\frac{1+\sqrt{5}}{2}\right)^2 + \alpha_2 \left(\frac{1-\sqrt{5}}{2}\right)^2 = 3$$

* There are two ways to solve this problem and get the value of α_1 & α_2:

(1) By substituting equations on each other.

(2) By Matrix: $Ax = B \rightsquigarrow x = A^{-1}B$

$$\begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ \left(\frac{1+\sqrt{5}}{2}\right)^2 & \left(\frac{1-\sqrt{5}}{2}\right)^2 \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix} \qquad (Ax = B)$$

$$\det(A) = \left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)^2 = \sqrt{5}$$

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} \left(\frac{1-\sqrt{5}}{2}\right)^2 & -\left(\frac{1-\sqrt{5}}{2}\right) \\ -\left(\frac{1+\sqrt{5}}{2}\right)^2 & \left(\frac{1+\sqrt{5}}{2}\right) \end{pmatrix} \begin{pmatrix} 2 \\ 3 \end{pmatrix} = \begin{pmatrix} \frac{3+\sqrt{5}}{2\sqrt{5}} \\ \frac{-3+\sqrt{5}}{2\sqrt{5}} \end{pmatrix}$$

Ex. Solve $a_n = 6a_{n-1} - 9a_{n-2}$ $\quad a_0 = 1, a_1 = 2$

Sol.

char eq. $r^2 - 6r - 9 = 0$

$$\text{roots} = \frac{6 \pm \sqrt{36 - 4 \times 9}}{2} = 3$$

$$a_n = (d_1 + d_2 n) \times 3^n$$

use I.C.

Generating Function (GF)

a way to
* Express a sequence using function.

sequence: $a_0, a_1, a_2, a_3, \cdots$

GF : $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$

sequence	GF
$\langle 0,0,0,\cdots\rangle$	0
$\langle 1,1,1,\cdots\rangle$	$1+x+x^2+x^3+\cdots$
$\langle 1,1,1,1,0,0,\cdots\rangle$	$1+x+x^2+x^3$, $\frac{x^4-1}{x-1}$

What is GF to generate $\langle 2,2,2,2,\cdots\rangle$:

$2 \times \langle 1,1,1,1,\cdots\rangle \rightarrow \frac{2}{1-x}$

$\langle \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \cdots\rangle \rightarrow \frac{1}{2} \cdot \frac{1}{1-x}$

$\langle 0,0,1,1,1,\cdots\rangle \quad \frac{x^2}{1-x}$

$0 + 0 \cdot x + x^2 + x^3 + x^4 + \cdots$

$x^2(1+x+x^2+\cdots)$

$x^2 \cdot \frac{1}{1-x} = \frac{x^2}{1-x}$

$\langle a_0, a_1, a_2, \cdots\rangle \rightarrow a_0 + a_1 x + a_2 x^2 + \cdots$ (open form)

$= \sum_{i=0}^{\infty} a_i x^i$

place holder

$\langle 1,1,1,1,\cdots\rangle \rightarrow 1 + x + x^2 + x^3 + \cdots$

$= \sum_{k=0}^{\infty} x^k$

* بسبب أن الـ x هي ، فلذلك لا يلزم فيتقرا 0

$= \lim_{n\to\infty} \sum_{k=0}^{n} x^k = \lim_{n\to\infty} \frac{x^{n+1} - 1}{x-1}$

$= \frac{1}{1-x}$ (closed form)

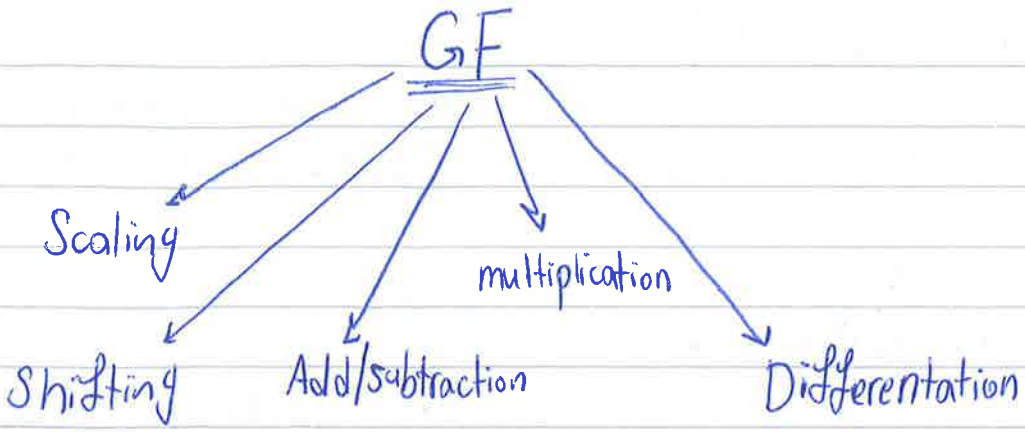
$\langle 1,1,1,1,\cdots\rangle \rightarrow \frac{1}{1-x}$

$\langle 0,0,0,0,1,1,1,\cdots\rangle \rightarrow \frac{x^4}{1-x}$

$\langle 1,1,1,1,0,0,0,\cdots\rangle \quad \frac{x^4-1}{x-1}$

$\langle 1,-1,1,-1,\cdots\rangle \rightarrow \frac{1}{1+x}$

$\langle 1,a,a^2,a^3,\cdots\rangle \rightarrow \frac{1}{1-ax}$



* Scaling:

$5x\langle 1,1,1,1,\dots\rangle \longrightarrow \frac{1}{1-x}$

$\langle 5,5,5,5,\dots\rangle \longrightarrow \frac{5}{1-x}$

$\langle \frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\dots\rangle \longrightarrow \frac{\frac{1}{2}}{1-x}$

* Shifting:

$\langle 1,1,1,1,\dots\rangle \longrightarrow \frac{1}{1-x}$

$\langle 0,1,1,1,\dots\rangle \longrightarrow \frac{x}{1-x}$

$\langle 0,0,1,1,1,\dots\rangle \longrightarrow \frac{x^2}{1-x}$

* Adding / Subtraction:

$$\langle 1,1,1,1,\cdots\rangle \longrightarrow \frac{1}{1-x}$$

$$-$$

$$\text{sub.}\quad \langle 0,0,0,1,1,\cdots\rangle \longrightarrow \frac{x^3}{1-x}$$

$$\langle 1,1,1,0,0,0,\cdots\rangle \longrightarrow \frac{1-x^3}{1-x}$$

$\langle 10,10,1,1,1,\cdots\rangle =$ أريد أن أصل إلى هذه المتتابعة

$$\frac{10(1-x^2)}{1-x} \longrightarrow \langle 10, 10, 0,0,0,\cdots\rangle$$

$$+$$

$$\text{Add.}\quad \frac{x^2}{1-x} \longrightarrow \langle 0,0,1,1,1,\cdots\rangle$$

$$\frac{10-9x^2}{1-x} \qquad \langle 10,10,1,1,1,\cdots\rangle$$

* Differentiation:

قانون مشتقة القسمة: $\frac{f(x)}{g(x)}$

$$\frac{f'(x)g(x)-f(x)g'(x)}{(g(x))^2}$$

$$\langle 1,1,1,\cdots\rangle \longrightarrow \frac{1}{1-x}$$

$$\Downarrow$$

$$\frac{d}{dx}(1+x+x^2+x^3+\cdots) \longrightarrow \frac{d}{dx}\left(\frac{1}{1-x}\right)$$ ← قانون اشتقاق القسمة

$$\downarrow$$

$$0+1+2x+3x^2+\cdots \longrightarrow \frac{1}{(1-x)^2}$$

$$\longrightarrow \langle 1,2,3,4,\cdots\rangle$$ ← GF

* Multiplication:

$\langle a_0, a_1, a_2, \cdots \rangle \longrightarrow A(x)$

$\langle b_0, b_1, b_2, \cdots \rangle \longrightarrow B(x)$

$C(x) = A(x) \times B(x)$

$\longrightarrow \langle \underbrace{a_0 b_0}_{c_0}, \underbrace{a_0 b_1 + a_1 b_0}_{c_1}, \underbrace{a_0 b_2 + a_1 b_1 + a_2 b_0}_{c_2}, \cdots \rangle$

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

$\langle c_0, c_1, c_2, \cdots \rangle$

$\langle 1, 1, 1, \cdots \rangle \longrightarrow \frac{1}{1-x}$

if you multiply it by itself:

$\langle 1, 1+1, 1+1+1, \cdots \rangle$

$\longrightarrow \langle 1, 2, 3, \cdots \rangle = \left(\frac{1}{1-x}\right)\left(\frac{1}{1-x}\right) = \frac{1}{(1-x)^2}$

Binomial Coeff.

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \qquad 0 \le k \le n \qquad k, n \in \mathbb{Z}^+$$

Extended Binomial coefficient $(u \in \mathbb{R},\ k \in \mathbb{Z}^+)$

$$\binom{u}{k} = \begin{cases} \dfrac{u(u-1)(u-2)\times \cdots \times (u-k+1)}{k!} & k > 0 \\ 1 & k = 0 \end{cases}$$

$$\binom{-2}{3} = \frac{(-2)\times(-3)\times(-4)}{3!} = -4$$

$$\binom{\frac{1}{2}}{3} = \frac{\frac{1}{2}\times\left(-\frac{1}{2}\right)\times\left(-\frac{3}{2}\right)}{3!} = \frac{1}{16} = 0.0625$$

Binomial Th.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \qquad n \ge 0$$

Extended Binomial Theorem

$$(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k \qquad u \in \mathbb{R} \qquad |x| < 1$$

↓

because if x is larger than 1 it will be exponential, and we want to decrease it.

Ex. Solve $(1+0.8)^{\frac{1}{2}}$.

Sol:

$$(1+0.8)^{\frac{1}{2}} = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} \times 0.8^k$$

$$= 1 + \underbrace{\binom{\frac{1}{2}}{1}}_{\frac{1}{2}} \times 0.8 + \underbrace{\binom{\frac{1}{2}}{2}}_{\frac{\frac{1}{2}\times(-\frac{1}{2})}{2} = -\frac{1}{8}} \times 0.8^2 + \underbrace{\binom{\frac{1}{2}}{3}}_{\frac{\frac{1}{2}\times(-\frac{1}{2})\times(-\frac{3}{2})}{3!} = \frac{3}{8\times 6} = \frac{1}{16}} \times 0.8^3 + \cdots$$

$$= \underbrace{1 + \tfrac{1}{2}\times 0.8}_{1.4} \underbrace{- \tfrac{1}{8}\times 0.8^2}_{1.336} + \underbrace{\tfrac{1}{16}\times 0.8^3}_{1.3616} + \cdots$$

$$\sqrt{1.8} = 1.3416407$$

(وهذا يدل على أن التابع كل ماله يقترب من $\sqrt{1.8}$)